

UNCLASSIFIED



McAfee VirusScan Managed Client

Version: 4

Release: 2

23 April 2010

STIG.DOD.MIL

Sort Order: [Group ID \(Vulid\), ascending order](#)

Notice: Developed by DISA for the DoD

Description:

CIRCLE ONE

FOR OFFICIAL USE ONLY (mark each page)

CONFIDENTIAL and SECRET (mark each page and each finding)

Classification is based on classification of system reviewed:

Unclassified System = FOUO Checklist

Confidential System = CONFIDENTIAL Checklist

Secret System= SECRET Checklist

Top Secret System = SECRET Checklist

Group ID (Vulid): [V-6453](#)

Group Title: DTAM001-McAfee VirusScan Control Panel

Rule ID: SV-23670r1_rule

Severity: CAT I

Rule Version (STIG-ID): DTAM001

Rule Title: The McAfee VirusScan Control Panel parameters are not configured as required.

Vulnerability Discussion: This parameter controls if the scan is started at startup.

Responsibility: System Administrator

Check Content:

Procedure: Use the Windows Registry Editor to navigate to the following key:
HKLM\Software\McAfee\VSCore\On access scanner\McShield\Configuration

Criteria: If the value of bStartDisabled is 0, this is not a finding. If the value is 1, this is a finding

Check Content:

From the ePO server console, select Systems tab, select the asset to be checked, select the Policies tab, select from the product pull down list VirusScan Enterprise 8.7.0. Locate in the Category column the On-Access General Policies. Select from the Policy column the policy associated with the On-Access General Policies. Under the General tab, locate the "Enable on-access scanning:" label. Ensure the "Enable on-access scanning at system startup" option is selected.

Criteria: If the "Enable on-access scanning at startup" option is selected this is not a finding.

Fix Text: From the ePO server console, select Systems Tab, select the asset to be checked, select the Policies tab, select from the product pull down list VirusScan Enterprise 8.7.0. Locate in the Category column the On-Access General Policies. Select from the Policy column the policy associated with the On-Access General Policies. Under the General tab, locate the "Enable on-access scanning:" label. Select the "Enable on-access scanning at system startup" option. Select Save.

Group ID (Vulid): [V-6467](#)

Group Title: DTAM002-McAfee VirusScan on access scan boot sect

Rule ID: SV-21320r1_rule

Severity: CAT II

Rule Version (STIG-ID): DTAM002

Rule Title: The McAfee VirusScan on access scan parameter for Boot sectors is incorrect.

Vulnerability Discussion: This parameter controls if boot sectors are scanned at startup.

Responsibility: System Administrator

Check Content:

From the ePO server console, select Systems tab, select the asset to be checked, select the Policies tab, select from the product pull down list VirusScan Enterprise 8.7.0. Locate in the Category column the On-Access General Policies. Select from the Policy column the policy associated with the On-Access General Policies. Under the General tab, locate the "Scan:" label. Ensure the "Boot Sectors" option is selected.

Criteria: If the "Boot Sectors" option is selected this is not a finding.

Check Content:

Procedure: Use the Windows Registry Editor to navigate to the following key:

HKLM\Software\McAfee\VSCore\On Access Scanner\Mcshield\configuration

Criteria: If the value of bDontScanBootSectors is 0, this is not a finding. If the value is 1, this is a finding.

Fix Text: From the ePO server console, select Systems tab, select the asset to be checked, select the Policies tab, select from the product pull down list VirusScan Enterprise 8.7.0. Locate in the Category column the On-Access General Policies. Select from the Policy column the policy associated with the On-Access General Policies. Under the General tab, locate the "Scan:" label. Select the "Boot Sectors" option. Select Save.

Group ID (Vulid): V-6468

Group Title: DTAM003-McAfee VirusScan on access scan floppy

Rule ID: SV-21321r1_rule

Severity: CAT II

Rule Version (STIG-ID): DTAM003

Rule Title: The McAfee VirusScan on access scan parameter for floppy disks is incorrect.

Vulnerability Discussion: This parameter controls the scanning of floppy disks.

Responsibility: System Administrator

Check Content:

From the ePO server console, select Systems tab, select the asset to be checked, select the Policies tab, select from the product pull down list VirusScan Enterprise 8.7.0. Locate in the Category column the On-Access General Policies. Select from the Policy column the policy associated with the On-Access General Policies. Under the General tab, locate the "Scan:" label. Ensure the "Floppy during shutdown" option is selected.

Criteria: If the " Floppy during shutdown " option is selected this is not a finding.

Check Content:

Procedure: Use the Windows Registry Editor to navigate to the following key:

HKLM\Software\McAfee\VSCore\On Access Scanner\mcshield\Configuration

Criteria: If the value of bScanFloppyonShutdown is 1, this is not a finding. If the value is 0, this is a finding

Fix Text: From the ePO server console, select Systems tab, select the asset to be checked, select the Policies tab, select from the product pull down list VirusScan Enterprise 8.7.0. Locate in the Category column the On-Access General Policies. Select from the Policy column the policy associated with the On-Access General Policies. Under the General tab, locate the "Scan:" label. Select the " Floppy during shutdown " option. Select Save.

Group ID (Vulid): V-6469

Group Title: DTAM004-McAfee VirusScan message dialog

Rule ID: SV-21322r1_rule

Severity: CAT II

Rule Version (STIG-ID): DTAM004

Rule Title: The McAfee VirusScan message dialog parameters are not configured as required.

Vulnerability Discussion: This parameter notifies the user when a virus is detected.

Responsibility: System Administrator

Check Content:

From the ePO server console, select Systems tab, select the asset to be checked, select the Policies tab, select from the product pull down list VirusScan Enterprise 8.7.0. Locate in the Category column the On-Access General Policies. Select from the Policy column the policy associated with the On-Access General Policies. Under the Messages tab, locate the "User message:" label. Ensure the "Show the messages dialog box when a threat is detected and display the specified text in the message" option is selected.

Criteria: If the "Show the messages dialog box when a threat is detected and display the specified text in the message" option is selected this is not a finding.

Check Content:

Procedure: Use the Windows Registry Editor to navigate to the following key:

HKLM\software\McAfee\VSCore\On access scanner\Mcshield\Configuration

Criteria: If the value of Alert_AutoShowList is 1, this is not a finding. If the value is 0, this is a finding.

Fix Text: From the ePO server console, select Systems tab, select the asset to be checked, select the Policies tab, select from the product pull down list VirusScan Enterprise 8.7.0. Locate in the Category column the On-Access General Policies. Select from the Policy column the policy associated with the On-Access General Policies. Under the Messages tab, locate the "User message:" label. Select the "Show the messages dialog box when a threat is detected and display the specified text in the message" option. Select Save.

Group ID (Vulid): V-6470

Group Title: DTAM005-McAfee VirusScan remove messages

Rule ID: SV-25546r1_rule

Severity: CAT II

Rule Version (STIG-ID): DTAM005

Rule Title: The McAfee VirusScan remove messages parameters are not configured as required.

Vulnerability Discussion: This parameter controls if users can remove virus alerts from the display.

Responsibility: System Administrator

Check Content:

Procedure: Use the Windows Registry Editor to navigate to the following key:

HKLM\Software\McAfee\VSCore\On Access Scanner\mcshield\Configuration

Criteria: If the value of Alert_UsersCanRemove is 0, this is not a finding. If the value is 1, this is a finding

Check Content:

From the ePO server console, select Systems tab, select the asset to be checked, select the Policies tab, select from the product pull down list VirusScan Enterprise 8.7.0. Locate in the Category column the On-Access General Policies. Select from the Policy column the policy associated with the On-Access General Policies. Under the Messages tab, locate the "Actions available to user:" label. Ensure the "Remove messages from the list" option is

NOT selected.

Criteria: If the "Remove messages from the list" option is NOT selected, this is not a finding.

Fix Text: From the ePO server console, select Systems tab, select the asset to be checked, select the Policies tab, select from the product pull down list VirusScan Enterprise 8.7.0. Locate in the Category column the On-Access General Policies. Select from the Policy column the policy associated with the On-Access General Policies. Under the Messages tab, locate the "Actions available to user:" label. Ensure the "Remove messages from the list" option is NOT selected. Select Save.

Group ID (Vulid): V-6471

Group Title: DTAM006-McAfee VirusScan Clean Infected file

Rule ID: SV-21323r1_rule

Severity: CAT II

Rule Version (STIG-ID): DTAM006

Rule Title: The McAfee VirusScan Clean Infected file parameter is not configured as required.

Vulnerability Discussion: This parameter determines if infected files are cleaned.

Responsibility: System Administrator

Check Content:

From the ePO server console, select Systems tab, select the asset to be checked, select the Policies tab, select from the product pull down list VirusScan Enterprise 8.7.0. Locate in the Category column the On-Access General Policies. Select from the Policy column the policy associated with the On-Access General Policies. Under the Messages tab, locate the "Actions available to user:" label. Ensure the "Clean files" option is selected.

Criteria: If the "Clean files" option is selected this is not a finding.

Check Content:

Procedure: Use the Windows Registry Editor to navigate to the following key:

HKLM\Software\Mcafee\VSCore\

On Access Scanner\mcshield\Configuration

Criteria: If the value of Alert_UsersCanClean is 1, this is not a finding. If the value is 0, this is a finding.

Fix Text: From the ePO server console, select Systems tab, select the asset to be checked, select the Policies tab, select from the product pull down list VirusScan Enterprise 8.7.0. Locate in the Category column the On-Access General Policies. Select from the Policy column the policy associated with the On-Access General Policies. Under the Messages tab, locate the "Actions available to user:" label. Select the "Clean files" option. Select Save.

Group ID (Vulid): V-6472

Group Title: DTAM007-McAfee VirusScan delete infected file

Rule ID: SV-21324r1_rule

Severity: CAT II

Rule Version (STIG-ID): DTAM007

Rule Title: The McAfee VirusScan delete infected file parameter is not configured as required.

Vulnerability Discussion: This parameter controls if infected files are deleted.

Responsibility: System Administrator

Check Content:

From the ePO server console, select Systems tab, select the asset to be checked, select the Policies tab, select from the product pull down list VirusScan Enterprise 8.7.0. Locate in the Category column the On-Access General Policies. Select from the Policy column the policy associated with the On-Access General Policies. Under the Messages tab, locate the "Actions available to user:" label. Ensure the "Delete files" option is selected.

Criteria: If the "Delete files" option is selected, this is not a finding.

Check Content:

Procedure: Use the Windows Registry Editor to navigate to the following key:

HKLM\Software\McAfee\VSCore\On Access Scanner\mcshield\Configuration

Criteria: If the value of Alert_UsersCanDelete is 1, this is not a finding. If the value is 0, this is a finding.

Fix Text: From the ePO server console, select Systems tab, select the asset to be checked, select the Policies tab, select from the product pull down list VirusScan Enterprise 8.7.0. Locate in the Category column the On-Access General Policies. Select from the Policy column the policy associated with the On-Access General Policies. Under the Messages tab, locate the "Actions available to user:" label. Select the "Delete files" option. Select Save.

Group ID (Vulid): V-6474

Group Title: DTAM009-McAfee VirusScan Control Panel log

Rule ID: SV-21325r1_rule

Severity: CAT II

Rule Version (STIG-ID): DTAM009

Rule Title: The McAfee VirusScan Control Panel log parameter is not configured as required.

Vulnerability Discussion: This parameter controls the logging of the scan.

Responsibility: System Administrator

Check Content:

From the ePO server console, select Systems tab, select the asset to be checked, select the Policies tab, select from the product pull down list VirusScan Enterprise 8.7.0. Locate in the Category column the On-Access General Policies. Select from the Policy column the policy associated with the On-Access General Policies. Under the Reports tab, locate the "Log to file:" label.

Criteria: If the "Enable activity logging and accept the default location for the log file or specify a new location" option is selected, this is not a finding.

Check Content:

Procedure: Use the Windows Registry Editor to navigate to the following key:

HKLM\Software\McAfee\VSCore\On Access Scanner\mcshield\Configuration

Criteria: If the value of bLogToFile is 1, this is not a finding. If the value is 0, this is a finding.

Fix Text: From the ePO server console, select Systems tab, select the asset to be checked, select the Policies tab, select from the product pull down list VirusScan Enterprise 8.7.0. Locate in the Category column the On-Access General Policies. Select from the Policy column the policy associated with the On-Access General Policies. Under the Reports tab, locate the "Log to file:" label. Select the "Enable activity logging and accept the default location for the log file or specify a new location" option. Select Save.

Group ID (Vulid): V-6475

Group Title: DTAM010-McAfee VirusScan limit log size parameter

Rule ID: SV-21326r1_rule

Severity: CAT II

Rule Version (STIG-ID): DTAM010

Rule Title: The McAfee VirusScan limit log size parameter is not configured as required.

Vulnerability Discussion: This parameter controls the log size.

Responsibility: System Administrator

Check Content:

From the ePO server console, select Systems tab, select the asset to be checked, select the Policies tab, select from the product pull down list VirusScan Enterprise 8.7.0. Locate in the Category column the On-Access General Policies. Select from the Policy column the policy associated with the On-Access General Policies. Under the Reports tab, locate the "Log file size" label.

Criteria: If the "Limit the size of the file" option is not selected, this is not a finding.

Criteria: If the "Limit the size of the file" option is selected and the "Maximum log file size:" is at least 100MB, this is not a finding.

Check Content:

Procedure: Use the Windows Registry Editor to navigate to the following key:

HKLM\Software\McAfee\VSCore\On Access Scanner\mcshield\Configuration

bLimitSize=1 and dwMaxLogSizeMB=x64 (100)

Criteria: If the value of bLimitSize is 1, and the dwMaxLogSizeMB is at least x64 (100)

or bLimitSize is 0, this is not a finding.

If the bLimitSize is 1 and dwMaxLogSizeMB is less than x64 (100), this is a finding.

Fix Text: From the ePO server console, select Systems tab, select the asset to be checked, select the Policies tab, select from the product pull down list VirusScan Enterprise 8.7.0. Locate in the Category column the On-Access General Policies. Select from the Policy column the policy associated with the On-Access General Policies. Under the Reports tab, locate the "Log file size:" label. IF the "Limit the size of the file" option is not to be used, ensure "Limit the size of the file" is not selected. If the "Limit the size of the file" option is selected, ensure the "Maximum log file size:" is at least 100MB.

Group ID (Vulid): V-6476

Group Title: DTAM011-McAfee VirusScan log session parameter

Rule ID: SV-21327r1_rule

Severity: CAT II

Rule Version (STIG-ID): DTAM011

Rule Title: The McAfee VirusScan log session parameter is not configured as required.

Vulnerability Discussion: This parameter controls if session settings are being logged.

Responsibility: System Administrator

Check Content:

From the ePO server console, select Systems tab, select the asset to be checked, select the Policies tab, select from the product pull down list VirusScan Enterprise 8.7.0. Locate in the Category column the On-Access General Policies. Select from the Policy column the policy associated with the On-Access General Policies. Under the Reports tab, locate the "What to log in addition to scanning activity" label. Ensure the "Session settings" option is selected.

Criteria: If the "Session settings" option is selected, this is not a finding.

Check Content:

Procedure: Use the Windows Registry Editor to navigate to the following key:
HKLM\Software\McAfee\VSCore\On Access Scanner\mcshield\Configuration
Criteria: If the value of bLogSettings is 1, this is not a finding. If the value is 0, this is a finding.

Fix Text: From the ePO server console, select Systems tab, select the asset to be checked, select the Policies tab, select from the product pull down list VirusScan Enterprise 8.7.0. Locate in the Category column the On-Access General Policies. Select from the Policy column the policy associated with the On-Access General Policies. Under the Reports tab, locate the "What to log in addition to scanning activity:" label. Select the "Session settings" option. Select Save.

Group ID (Vulid): [V-6478](#)

Group Title: DTAM012-McAfee VirusScan log summary parameter

Rule ID: SV-21328r1_rule

Severity: CAT II

Rule Version (STIG-ID): DTAM012

Rule Title: The McAfee VirusScan log summary parameter is not configured as required.

Vulnerability Discussion: This parameter controls if the session summary is being logged.

Responsibility: System Administrator

Check Content:

From the ePO server console, select Systems tab, select the asset to be checked, select the Policies tab, select from the product pull down list VirusScan Enterprise 8.7.0. Locate in the Category column the On-Access General Policies. Select from the Policy column the policy associated with the On-Access General Policies. Under the Reports tab, locate the "What to log in addition to scanning activity" label. Ensure the "Session summary" option is selected.

Criteria: If the "Session summary" option is selected, this is not a finding.

Check Content:

Procedure: Use the Windows Registry Editor to navigate to the following key:
HKLM\Software\McAfee\VSCore\On Access Scanner\mcshield\Configuration
Criteria: If the value of bLogSummary is 1, this is not a finding. If the value is 0, this is a finding.

Fix Text: From the ePO server console, select Systems tab, select the asset to be checked, select the Policies tab, select from the product pull down list VirusScan Enterprise 8.7.0. Locate in the Category column the On-Access General Policies. Select from the Policy column the policy associated with the On-Access General Policies. Under the Reports tab, locate the "What to log in addition to scanning activity:" label. Select the "Session summary" option. Select Save.

Group ID (Vulid): [V-6583](#)

Group Title: DTAM013-McAfee VirusScan log encrypted files param

Rule ID: SV-21329r1_rule

Severity: CAT II

Rule Version (STIG-ID): DTAM013

Rule Title: The McAfee VirusScan log encrypted files parameter is not configured as required.

Vulnerability Discussion: This parameter controls if failure to scan encrypted files is logged.

Responsibility: System Administrator

Check Content:

From the ePO server console, select Systems tab, select the asset to be checked, select the Policies tab, select from the product pull down list VirusScan Enterprise 8.7.0. Locate in the Category column the On-Access General Policies. Select from the Policy column the policy associated with the On-Access General Policies. Under the Reports tab, locate the "What to log in addition to scanning activity" label. Ensure the "Failure to scan encrypted files" option is selected.

Criteria: If the "Failure to scan encrypted files" option is selected, this is not a finding.

Check Content:

Use the Windows Registry Editor to navigate to the following key:
HKLM\Software\Network Associates\TVD\Shared Components\On Access
Scanner\mcshield\Configuration

Criteria: If the value ReportEncryptedFiles is 1, this is not a finding. If the value is 0, this is a finding.

Fix Text: From the ePO server console, select Systems tab, select the asset to be checked, select the Policies tab, select from the product pull down list VirusScan Enterprise 8.7.0. Locate in the Category column the On-Access General Policies. Select from the Policy column the policy associated with the On-Access General Policies. Under the Reports tab, locate the "What to log in addition to scanning activity:" label. Select the "Failure to scan encrypted files" option. Select Save.

Group ID (Vulid): V-6585

Group Title: DTAM016-McAfee VirusScan autoupdate parameters

Rule ID: SV-21337r1_rule

Severity: CAT II

Rule Version (STIG-ID): DTAM016

Rule Title: The McAfee VirusScan autoupdate parameters are not configured as required.

Vulnerability Discussion: This parameter ensure that the product is configured to get autoupdates.

Responsibility: System Administrator

Check Content:

From the ePO server console, select Systems tab, select the asset to be checked, select Client Tasks tab. From the list of available tasks in the Task Name column, identify the scheduled update task. In the Product Name column, ensure that McAfee Agent is selected, in the Status column, ensure that the status is Enabled; and in the Schedule column, ensure that the update is scheduled on at least a weekly basis.

Criteria: If a McAfee Agent update is Enabled and scheduled for at least a weekly update this is not a finding.

On the client machine use the Windows Explorer to navigate to the following folder:

%SystemDrive%\Document and Settings\All Users\Application Data\McAfee\Common Framework\Task\.

Multiple .ini files will be stored in this folder one for each task defined on the ePO server for this client. The name for each task is identified in the first section of the file under the [Task] section on the TaskName= "" line.

Additionally, a TaskType= line in the [General] section of the file is provided to describe the task type. In this case TaskType=update is expected. Information for this check is determined by examining the contents of this file.

Criteria:

If [Settings] Enabled=1 and [Schedule] Type=0 the schedule is daily, this is not a finding.

If [Settings] Enabled=1 and [Schedule] Type=1 the schedule is weekly, this is not a finding.

Fix Text: From the ePO server console, select Systems tab, select Client Tasks tab, select New Task. On the Description page, provide a descriptive Name:, select Update (McAfee Agent) from the Type: pull down menu, and select Next. On the Configuration page in the Signatures and engines: section, ensure that Engine and DAT are selected, and select Next. On the Schedule page in the Schedule status: section, ensure Enabled is selected; in the Schedule type: section, ensure that at least Weekly is selected, and select Next. On the Summary page, select Save. Update client machine.

Group ID (Vulid): [V-6586](#)

Group Title: DTAM021-McAfee VirusScan Exchange scanner

Rule ID: SV-21339r1_rule

Severity: CAT II

Rule Version (STIG-ID): DTAM021

Rule Title: The McAfee VirusScan Exchange scanner is not enabled.

Vulnerability Discussion: This parameter controls if the email client scanner is active.

Responsibility: System Administrator

Check Content:

From the ePO server console, select Systems tab, select the asset to be checked, select the Policies tab, select from the product pull down list VirusScan Enterprise 8.7.0. Locate in the Category column the On Delivery Email Scan Policies. Select from the Policy column the policy associated with the On Delivery Email Scan Policies. Under the Scan Items tab, locate the "Scanning of email:" label. Ensure the "Enable on-delivery email scanning" option is selected.

Criteria: If the "Enable on-delivery email scanning" is selected, this is not a finding.

Check Content:

Procedure: Use the Windows Registry Editor to navigate to the following key:

HKLM\Software\McAfee\VSCore\Email Scanner\Outlook\OnDelivery\GeneralOptions

Criteria: If the value bEnabled is 1, this is not a finding.

Fix Text: From the ePO server console, select Systems tab, select the asset to be checked, select the Policies tab, select from the product pull down list VirusScan Enterprise 8.7.0. Locate in the Category column the On Delivery Email Scan Policies. Select from the Policy column the policy associated with the On Delivery Email Scan Policies. Under the Scan Items tab, locate the "Scanning of email:" label. Select the "Enable on-delivery email scanning" option. Select Save.

Group ID (Vulid): [V-6587](#)

Group Title: DTAM022-McAfee VirusScan find unknown programs

Rule ID: SV-21341r1_rule

Severity: CAT II

Rule Version (STIG-ID): DTAM022

Rule Title: The McAfee VirusScan find unknown programs email parameter is not configured as required.

Vulnerability Discussion: This parameter controls if scanning is performed for unknown program viruses.

Responsibility: System Administrator

Check Content:

From the ePO server console, select Systems tab, select the asset to be checked, select the Policies tab, select from the product pull down list VirusScan Enterprise 8.7.0. Locate in the Category column the On Delivery Email Scan Policies. Select from the Policy column the policy associated with the On Delivery Email Scan Policies. Under the

Scan Items tab, locate the "Heuristics:" label. Ensure the "Find unknown program threats and trojans" option is selected.

Criteria: If the "Find unknown program threats and trojans" option is selected, this is not a finding.

Check Content:

Procedure: Use the Windows Registry Editor to navigate to the following key:

HKLM\Software\McAfee\VSCore\Email Scanner\Outlook\OnDelivery\DetectionOptions

Criteria: If the value dwProgramHeuristicsLevel is 1, this is not a finding. If the value is 0, this is a finding.

Fix Text: From the ePO server console, select Systems tab, select the asset to be checked, select the Policies tab, select from the product pull down list VirusScan Enterprise 8.7.0. Locate in the Category column the On Delivery Email Scan Policies. Select from the Policy column the policy associated with the On Delivery Email Scan Policies. Under the Scan Items tab, locate the "Heuristics:" label. Select the "Find unknown program threats and trojans" option. Select Save.

Group ID (Vulid): [V-6588](#)

Group Title: DTAM023- McAfee VirusScan find unknown macro virus

Rule ID: SV-21343r1_rule

Severity: CAT II

Rule Version (STIG-ID): DTAM023

Rule Title: The McAfee VirusScan find unknown macro virus email parameter is not configured as required.

Vulnerability Discussion: This parameter controls the scanning for unknown macro viruses.

Responsibility: System Administrator

Check Content:

From the ePO server console, select Systems tab, select the asset to be checked, select the Policies tab, select from the product pull down list VirusScan Enterprise 8.7.0. Locate in the Category column the On Delivery Email Scan Policies. Select from the Policy column the policy associated with the On Delivery Email Scan Policies. Under the Scan Items tab, locate the "Heuristics:" label. Ensure the "Find unknown macro threats" option is selected.

Criteria: If the "Find unknown macro threats" option is selected, this is not a finding.

Check Content:

Procedure: Use the Windows Registry Editor to navigate to the following key:

HKLM\Software\McAfee\VSCore\Email scanner\Outlook\OnDelivery\DetectionOptions

Criteria: If the value dwMacroHeuristicsLevel is 1, this is not a finding. If the value is 0, this is a finding.

Fix Text: From the ePO server console, select Systems tab, select the asset to be checked, select the Policies tab, select from the product pull down list VirusScan Enterprise 8.7.0. Locate in the Category column the On Delivery Email Scan Policies. Select from the Policy column the policy associated with the On Delivery Email Scan Policies. Under the Scan Items tab, locate the "Heuristics:" label. Select the "Find unknown macro threats" option. Select Save.

Group ID (Vulid): [V-6589](#)

Group Title: DTAM026-McAfee VirusScan scan inside archives email

Rule ID: SV-21344r1_rule

Severity: CAT II**Rule Version (STIG-ID):** DTAM026**Rule Title:** The McAfee VirusScan scan inside archives email parameter is not configured as required.**Vulnerability Discussion:** This parameter controls if the contents of archives are checked for viruses.**Responsibility:** System Administrator**Check Content:**

From the ePO server console, select Systems tab, select the asset to be checked, select the Policies tab, select from the product pull down list VirusScan Enterprise 8.7.0. Locate in the Category column the On Delivery Email Scan Policies. Select from the Policy column the policy associated with the On Delivery Email Scan Policies. Under the Scan Items tab, locate the "Compressed files:" label. Ensure the "Scan inside archives (e.g. .ZIP)" option is selected.

Criteria: If the "Scan inside archives (e.g. .ZIP)" option is selected, this is not a finding.

Check Content:

Procedure: Use the Windows Registry Editor to navigate to the following key:

HKLM\Software\McAfee\VSCore\Email scanner\Outlook\OnDelivery\DetectionOptions

Criteria: If the value ScanArchives is 1, this is not a finding. If the value is 0, this is a finding.

Fix Text: From the ePO server console, select Systems tab, select the asset to be checked, select the Policies tab, select from the product pull down list VirusScan Enterprise 8.7.0. Locate in the Category column the On Delivery Email Scan Policies. Select from the Policy column the policy associated with the On Delivery Email Scan Policies. Under the Scan Items tab, locate the "Compressed files:" label. Select the "Scan inside archives (e.g. .ZIP)" option. Select Save.

Group ID (Vulid): [V-6590](#)**Group Title:** DTAM027-McAfee VirusScan decode MIME email**Rule ID:** SV-21345r1_rule**Severity: CAT II****Rule Version (STIG-ID):** DTAM027**Rule Title:** The McAfee VirusScan decode MIME email parameter is not configured as required.**Vulnerability Discussion:** This parameter controls if encoded files should be decoded for virus scans.**Responsibility:** System Administrator**Check Content:**

From the ePO server console, select Systems tab, select the asset to be checked, select the Policies tab, select from the product pull down list VirusScan Enterprise 8.7.0. Locate in the Category column the On Delivery Email Scan Policies. Select from the Policy column the policy associated with the On Delivery Email Scan Policies. Under the Scan Items tab, locate the "Compressed files:" label. Ensure the "Decode MIME encoded files" option is selected.

Criteria: If the "Decode MIME encoded files" option is selected, this is not a finding.

Check Content:

Procedure: Use the Windows Registry Editor to navigate to the following key:

HKLM\Software\McAfee\VSCore\Email Scanner\Outlook\OnDelivery\DetectionOptions

Criteria: If the value ScanMime is 1, this is not a finding. If the value is 0, this is a finding.

Fix Text: From the ePO server console, select Systems tab, select the asset to be checked, select the Policies tab, select from the product pull down list VirusScan Enterprise 8.7.0. Locate in the Category column the On Delivery Email Scan Policies. Select from the Policy column the policy associated with the On Delivery Email Scan Policies. Under the Scan Items tab, locate the "Compressed files:" label. Select the "Decode MIME encoded files" option.

Select Save.

Group ID (Vulid): V-6591

Group Title: DTAM028-McAfee VirusScan scan e-mail message body

Rule ID: SV-21346r1_rule

Severity: CAT II

Rule Version (STIG-ID): DTAM028

Rule Title: The McAfee VirusScan scan e-mail message body email parameter is not configured as required.

Vulnerability Discussion: This parameter ensures the email message contents is scanned for viruses.

Responsibility: System Administrator

Check Content:

From the ePO server console, select Systems tab, select the asset to be checked, select the Policies tab, select from the product pull down list VirusScan Enterprise 8.7.0. Locate in the Category column the On Delivery Email Scan Policies. Select from the Policy column the policy associated with the On Delivery Email Scan Policies. Under the Scan Items tab, locate the "Email message body (for Microsoft Outlook only):" label. Ensure the "Scan email message body" option is selected.

Criteria: If the option "Scan email message body" is selected, this is not a finding.

Check Content:

Procedure: Use the Windows Registry Editor to navigate to the following key:

HKLM\Software\McAfee\VSCore\Email scanner\outlook\onDelivery\DetectionOptions

Criteria: If the value ScanMessageBodies is 1, this is not a finding. If the value is 0, this is a finding.

Fix Text: From the ePO server console, select Systems tab, select the asset to be checked, select the Policies tab, select from the product pull down list VirusScan Enterprise 8.7.0. Locate in the Category column the On Delivery Email Scan Policies. Select from the Policy column the policy associated with the On Delivery Email Scan Policies. Under the Scan Items tab, locate the "Email message body (for Microsoft Outlook only):" label. Select the "Scan email message body" option. Select Save.

Group ID (Vulid): V-6592

Group Title: DTAM029-McAfee VirusScan allowed actions email

Rule ID: SV-21347r1_rule

Severity: CAT II

Rule Version (STIG-ID): DTAM029

Rule Title: The McAfee VirusScan allowed actions email parameter is not configured as required.

Vulnerability Discussion: This parameter controls what actions should happen when a virus is detected.

Responsibility: System Administrator

Check Content:

From the ePO server console, select Systems tab, select the asset to be checked, select the Policies tab, select from the product pull down list VirusScan Enterprise 8.7.0. Locate in the Category column the On Delivery Email Scan Policies. Select from the Policy column the policy associated with the On Delivery Email Scan Policies. Under the Actions tab, locate the "When a threat is found:" section. In the "Perform this action first:" pull down menu, select the "Prompt for action" option.

Criteria: If the option "Prompt for action" is selected this is not a finding.

Check Content:

Procedure: Use the Windows Registry Editor to navigate to the following key:

HKLM\Software\McAfee\VSCore\Email Scanner\Outlook\OnDelivery\ActionOptions

Criteria: If the value uAction is 2, this is not a finding. If the value is other than 2, this is a finding.

Fix Text: From the ePO server console, select Systems tab, select the asset to be checked, select the Policies tab, select from the product pull down list VirusScan Enterprise 8.7.0. Locate in the Category column the On Delivery Email Scan Policies. Select from the Policy column the policy associated with the On Delivery Email Scan Policies. Under the Actions tab, locate the "When a threat is found:" section. In the "Perform this action first:" pull down menu, select the "Prompt for action" option. Select Save.

Group ID (Vulid): [V-6593](#)

Group Title: DTAM030-McAfee VirusScan action prompt email

Rule ID: SV-21348r1_rule

Severity: CAT II

Rule Version (STIG-ID): DTAM030

Rule Title: The McAfee VirusScan action prompt email parameter is not configured as required.

Vulnerability Discussion: This parameter ensures appropriate actions are prompted for when a virus is found.

Responsibility: System Administrator

Check Content:

From the ePO server console, select Systems tab, select the asset to be checked, select the Policies tab, select from the product pull down list VirusScan Enterprise 8.7.0. Locate in the Category column the On Delivery Email Scan Policies. Select from the Policy column the policy associated with the On Delivery Email Scan Policies. Under the Actions tab, locate the "Allowed actions in Prompt dialog box:" section, ensure that Clean attachment, Delete attachment, and Move attachment are selected.

Criteria: If the options "Clean attachment, Delete attachment, and Move attachment" are selected, this is not a finding.

Check Content:

Procedure: Use the Windows Registry Editor to navigate to the following key:

HKLM\Software\McAfee\VSCore\Email scanner\Outlook\OnDelivery\ActionOptions

Criteria: If the value dwPromptButton is x1F (31), this is not a finding. If the value is not x1F (31), this is a finding.

Fix Text: From the ePO server console, select Systems tab, select the asset to be checked, select the Policies tab, select from the product pull down list VirusScan Enterprise 8.7.0. Locate in the Category column the On Delivery Email Scan Policies. Select from the Policy column the policy associated with the On Delivery Email Scan Policies. Under the Actions tab, locate the "Allowed actions in Prompt dialog box:" section. Select the Clean attachment, Delete attachment, and Move attachment options. Select Save.

Group ID (Vulid): [V-6594](#)

Group Title: DTAM033-McAfee VirusScan return reply email

Rule ID: SV-21349r1_rule

Severity: CAT II

Rule Version (STIG-ID): DTAM033

Rule Title: The McAfee VirusScan return reply email parameter is not configured as required.

Vulnerability Discussion: This parameter controls if an email is sent back to the original email sender indicating there was a virus detected.

Responsibility: System Administrator

Check Content:

From the ePO server console, select Systems tab, select the asset to be checked, select the Policies tab, select from the product pull down list VirusScan Enterprise 8.7.0. Locate in the Category column the On Delivery Email Scan Policies. Select from the Policy column the policy associated with the On Delivery Email Scan Policies. Under the Alerts tab, locate the "Email alert for user:" section and ensure that "Send alert mail to user" is selected.

Criteria: If the option "Send alert mail to user" is selected, this is not a finding.

Check Content:

Procedure: Use the Windows Registry Editor to navigate to the following key:

HKLM\Software\McAfee\VSCore\Email Scanner\Outlook\OnDelivery\AlertOptions

Criteria: If the value bDisplayMessage is 1, this is not a finding. If the value is 0, this is a finding.

Fix Text: From the ePO server console, select Systems tab, select the asset to be checked, select the Policies tab, select from the product pull down list VirusScan Enterprise 8.7.0. Locate in the Category column the On Delivery Email Scan Policies. Select from the Policy column the policy associated with the On Delivery Email Scan Policies. Under the Alerts tab, locate the "Email alert for user:" section. Select the "Send alert mail to user" option. Select Save.

Group ID (Vulid): V-6595

Group Title: DTAM034- McAfee VirusScan prompt message email

Rule ID: SV-21350r1_rule

Severity: CAT II

Rule Version (STIG-ID): DTAM034

Rule Title: The McAfee VirusScan prompt message email parameter is not configured as required.

Vulnerability Discussion: This parameter ensures an appropriate message is displayed for the user to indicate a virus was found within an email.

Responsibility: System Administrator

Check Content:

From the ePO server console, select Systems tab, select the asset to be checked, select the Policies tab, select from the product pull down list VirusScan Enterprise 8.7.0. Locate in the Category column the On Delivery Email Scan Policies. Select from the Policy column the policy associated with the On Delivery Email Scan Policies. Under the Alerts tab, locate the "Prompt for action message:" section and ensure that "Specify the message that displays to the user when prompting for action. The Prompt for action option must be selected on the Actions tab. Accept the default message or type a new message." is selected.

Criteria: If the option "Specify the message that displays to the user when prompting for action. The Prompt for action option must be selected on the Actions tab. Accept the default message or type a new message." is selected, this is not a finding.

Check Content:

Procedure: Use the Windows Registry Editor to navigate to the following key:

HKLM\Software\McAfee\VSCore\Email Scanner\Outlook\OnDelivery\AlertOptions --

Criteria: If the value szCustomMessage contains an appropriate alert message, this is not a finding. If the value is blank or does not convey an alert, this is a finding.

Fix Text: From the ePO server console, select Systems tab, select the asset to be checked, select the Policies tab, select from the product pull down list VirusScan Enterprise 8.7.0. Locate in the Category column the On Delivery Email Scan Policies. Select from the Policy column the policy associated with the On Delivery Email Scan Policies. Under the Alerts tab, locate the "Prompt for action message:" section, select "Specify the message that displays to the user when prompting for action. The Prompt for action option must be selected on the Actions tab. Accept the default message or type a new message." Select Save.

Group ID (Vulid): [V-6596](#)

Group Title: DTAM035-McAfee VirusScan log to file email

Rule ID: SV-21351r1_rule

Severity: CAT II

Rule Version (STIG-ID): DTAM035

Rule Title: The McAfee VirusScan log to file email parameter is not configured as required.

Vulnerability Discussion: This parameter ensures that virus scanning sessions for email are logged.

Responsibility: System Administrator

Check Content:

From the ePO server console, select Systems tab, select the asset to be checked, select the Policies tab, select from the product pull down list VirusScan Enterprise 8.7.0. Locate in the Category column the On Delivery Email Scan Policies. Select from the Policy column the policy associated with the On Delivery Email Scan Policies. Under the Reports tab, locate the "Log to file:" section and ensure that "Enable activity logging and accept the default location for the log file or specify a new location." is selected.

Criteria: If the option "Enable activity logging and accept the default location for the log file or specify a new location." is selected, this is not a finding.

Check Content:

Procedure: Use the Windows Registry Editor to navigate to the following key:

HKLM\Software\McAfee\VSCore\Email Scanner\Outlook\OnDelivery\ReportOptions --

Criteria: If the value bLogToFile is 1, this is not a finding. If the value is 0, this is a finding.

Fix Text: From the ePO server console, select Systems tab, select the asset to be checked, select the Policies tab, select from the product pull down list VirusScan Enterprise 8.7.0. Locate in the Category column the On Delivery Email Scan Policies. Select from the Policy column the policy associated with the On Delivery Email Scan Policies. Under the Reports tab, locate the "Log to file:" section and select "Enable activity logging and accept the default location for the log file or specify a new location." Select Save.

Group ID (Vulid): [V-6597](#)

Group Title: DTAM036-McAfee VirusScan limit log size email

Rule ID: SV-21354r1_rule

Severity: CAT II

Rule Version (STIG-ID): DTAM036

Rule Title: The McAfee VirusScan limit log size email parameter is not configured as required.

Vulnerability Discussion: This parameter determines the size of the log file to ensure data is available for review.

Responsibility: System Administrator

Check Content:

From the ePO server console, select Systems tab, select the asset to be checked, select the Policies tab, select from the product pull down list VirusScan Enterprise 8.7.0. Locate in the Category column the On delivery Email Scan Policies. Select from the Policy column the policy associated with the On delivery Email Scan Policies. Under the Reports tab, locate the "Log file size" label.

Criteria: If the "Limit the size of the file" option is not selected, this is not a finding.

Criteria: If the "Limit the size of the file" option is selected and the "Maximum log file size:" is at least 100MB this is not a finding.

Check Content:

Procedure: Use the Windows Registry Editor to navigate to the following key:

HKLM\Software\McAfee\VSCore\Email Scanner\Outlook\OnDelivery\ReportOptions --

Criteria: If the value of bLimitSize is 1, and the dwMaxLogSizeMB is at least Hex 64 (100) or bLimitSize is 0 this is not a finding. If the bLimitSize is 0 or if dwMaxLogSizeMB is less than Hex 64, (100) this is a finding.

Fix Text: From the ePO server console, select Systems tab, select the asset to be checked, select the Policies tab, select from the product pull down list VirusScan Enterprise 8.7.0. Locate in the Category column the On Delivery Email Policies. Select from the Policy column the policy associated with the On Delivery Email Scan Policies. Under the Reports tab, locate the "Log file size:" label. If the "Limit the size of the file" option is not to be used, ensure "Limit the size of the file" is not selected. If the "Limit the size of the file" option is selected, ensure the "Maximum log file size:" is at least 100MB.

Group ID (Vulid): [V-6598](#)

Group Title: DTAM037-McAfee VirusScan log content email

Rule ID: SV-21352r1_rule

Severity: CAT II

Rule Version (STIG-ID): DTAM037

Rule Title: The McAfee VirusScan log content email parameter is not configured as required.

Vulnerability Discussion: This setting controls the entries that are stored in the virus scanning log.

Responsibility: System Administrator

Check Content:

From the ePO server console, select Systems tab, select the asset to be checked, select the Policies tab, select from the product pull down list VirusScan Enterprise 8.7.0. Locate in the Category column the On Delivery Email Policies. Select from the Policy column the policy associated with the On Delivery Email Policies. Under the Reports tab, locate the "What to log in addition to scanning activity" label. Ensure the "Session settings", "Session summary", and "Failure to scan encrypted files", options are selected.

Criteria: If the "Session settings", "Session summary", and "Failure to scan encrypted files", options are selected, this is not a finding.

Check Content:

Procedure: Use the Windows Registry Editor to navigate to the following key:

HKLM\Software\McAfee\VSCore\Email Scanner\Outlook\OnDelivery\ReportOptions. --

Criteria: If the value dwLogEvent is x130 (304), this is not a finding. If the value, is not x130 (304), this is a finding.

Fix Text: From the ePO server console, select Systems tab, select the asset to be checked, select the Policies tab, select from the product pull down list VirusScan Enterprise 8.7.0. Locate in the Category column the On Delivery

Email Policies. Select from the Policy column the policy associated with the On Delivery Email Policies. Under the Reports tab, locate the "What to log in addition to scanning activity:" label. Select the "Session settings", "Session summary", and "Failure to scan encrypted files", options. Select Save.

Group ID (Vulid): [V-6599](#)

Group Title: DTAM045-McAfee VirusScan fixed disk and processes

Rule ID: SV-21353r1_rule

Severity: CAT II

Rule Version (STIG-ID): DTAM045

Rule Title: The McAfee VirusScan fixed disk and running processes are not configured as required.

Vulnerability Discussion: This parameter ensures that all fixed disks and running processes are scanned for viruses.

Responsibility: System Administrator

Check Content:

From the ePO server console, select Systems tab, select the asset to be checked, select Client Tasks tab. From the list of available tasks in the Task Name column, with the assistance of the ePO SA, identify the weekly on demand client scan task. A daily or weekly on demand client scan may also be identified by reviewing the Product Name, Status, and Schedule of each Task Name in the Client Tasks window. In the same row as the on demand client scan task under review ensure that the Product Name column contains VirusScan Enterprise 8.7.0 and in the Status column, ensure that the status is Enabled. Select edit from the Actions column. In the Description tab, ensure that for "Type:" "On Demand Scan (VirusScan Enterprise 8.7.0)" is selected. Select the Configuration tab. Under the Scan Locations tab in Locations to scan: area, ensure that "All fixed drives" and "Running processes" are displayed.

Criteria: If "All fixed drives" and "Running processes" are displayed in the configuration for the daily or weekly On Demand Scan, this is not a finding.

On the client machine use the Windows Explorer to navigate to the following folder:

%SystemDrive%\Document and Settings\All Users\Application Data\McAfee\Common Framework\Task\.

Multiple .ini files will be stored in this folder one for each task defined on the ePO server for this client. The name for each task is identified in the first section of the file under the [Task] section on the TaskName= "" line.

Additionally, a TaskType= line in the [General] section of the file is provided to describe the type of scan. In this case TaskType=VSC700_Scan_Task is expected. Information for this check is determined by examining the contents of this file.

Criteria: If [ScanItems] szScanItemX=All fixed disks, and [Settings] scScanItemX=Special Memory are present, this is not a finding. : For the values of szScanItemX, the character X represents some integer =>0. Example: szScanItem0=All fixed disks, szScanItem1=Special Memory,

Fix Text: From the ePO server console, select Systems tab, select the asset to be checked, select Client Tasks tab. From the list of available tasks in the Task Name column, with the assistance of the ePO SA, identify the daily or weekly on demand client scan task. In the same row as the on demand client scan task ensure that the Product Name column contains VirusScan Enterprise 8.7.0, in the Status column ensure that the status is Enabled. Select edit from the Actions column. In the Description tab, ensure that for "Type:" "On Demand Scan (VirusScan Enterprise 8.7.0)" is selected. Select the Configuration tab. Under the Scan Locations tab in Locations to scan: area, from the pull down menus, select "All fixed drives" and "Running processes". Select Save.

Group ID (Vulid): [V-6600](#)

Group Title: DTAM046-McAfee VirusScan include subfolders

Rule ID: SV-21355r1_rule

Severity: CAT II

Rule Version (STIG-ID): DTAM046

Rule Title: The McAfee VirusScan include subfolders parameter is not configured as required.

Vulnerability Discussion: This parameter ensures that subfolders are scanned for viruses.

Responsibility: System Administrator

Check Content:

From the ePO server console, select Systems tab, select the asset to be checked, select Client Tasks tab. From the list of available tasks in the Task Name column, with the assistance of the ePO SA, identify the weekly on demand client scan task. A daily or weekly on demand client scan may also be identified by reviewing the Product Name, Status, and Schedule of each Task Name in the Client Tasks window. In the same row as the on demand client scan task under review, ensure that the Product Name column contains VirusScan Enterprise 8.7.0 and in the Status column, ensure that the status is Enabled. Select edit from the Actions column. In the Description tab ensure that for "Type:" "On Demand Scan (VirusScan Enterprise 8.7.0)" is selected. Select the Configuration tab. Under the Scan Locations tab, Scan options area, ensure that "Include subfolders" is displayed.

Criteria: If "Include subfolders" is displayed, this is not a finding.

On the client machine, use the Windows Explorer to navigate to the following folder:

%SystemDrive%\Document and Settings\All Users\Application Data\McAfee\Common Framework\Task\.

Multiple .ini files will be stored in this folder one for each task defined on the ePO server for this client. The name for each task is identified in the first section of the file under the [Task] section on the TaskName= "" line.

Additionally, a TaskType= line in the [General] section of the file is provided to describe the type of scan. In this case, TaskType=VSC700_Scan_Task is expected. Information for this check is determined by examining the contents of this file.

Criteria: If [Where] bScanSubDirs=1, this is not a finding.

Fix Text: From the ePO server console, select Systems tab, select the asset to be checked, select Client Tasks tab. From the list of available tasks in the Task Name column, with the assistance of the ePO SA, identify the weekly on demand client scan task. In the same row as the on demand client scan task, ensure that the Product Name column contains VirusScan Enterprise 8.7.0 and in the Status column, ensure that the status is Enabled. Select Edit from the Actions column. In the Description tab, ensure that for "Type:" "On Demand Scan (VirusScan Enterprise 8.7.0)" is selected. Select the Configuration tab. Under the Scan Locations tab, Scan options area, select "Include subfolders". Select Save.

Group ID (Vulid): V-6601

Group Title: DTAM047-McAfee VirusScan include boot sectors

Rule ID: SV-21356r1_rule

Severity: CAT II

Rule Version (STIG-ID): DTAM047

Rule Title: The McAfee VirusScan include boot sectors parameter is not configured as required.

Vulnerability Discussion: This parameter ensures that the boot sector is scanned for viruses.

Responsibility: System Administrator

Check Content:

From the ePO server console, select Systems tab, select the asset to be checked, select Client Tasks tab. From the list of available tasks in the Task Name column, with the assistance of the ePO SA, identify the weekly on demand client scan task. A daily or weekly on demand client scan may also be identified by reviewing the Product Name, Status, and Schedule of each Task Name in the Client Tasks window. In the same row as the on demand client scan

task under review, ensure that the Product Name column contains VirusScan Enterprise 8.7.0, in the Status column ensure that the status is Enabled. Select Edit from the Actions column. In the Description tab, ensure that for “Type:” “On Demand Scan (VirusScan Enterprise 8.7.0)” is selected. Select the Configuration tab. Under the Scan Locations tab, Scan options area, ensure that “Scan boot sectors” is displayed.

Criteria: If “Scan boot sectors” is displayed, this is not a finding.

On the client machine, use the Windows Explorer to navigate to the following folder:

%SystemDrive%\Document and Settings\All Users\Application Data\McAfee\Common Framework\Task\.

Multiple .ini files will be stored in this folder one for each task defined on the ePO server for this client. The name for each task is identified in the first section of the file under the [Task] section on the TaskName= “” line.

Additionally, a TaskType= line in the [General] section of the file is provided to describe the type of scan. In this case, TaskType=VSC700_Scan_Task is expected. Information for this check is determined by examining the contents of this file.

Criteria: If [Where] bSkipBootScan=0, this is not a finding.

Fix Text: From the ePO server console, select Systems tab, select the asset to be checked, select Client Tasks tab. From the list of available tasks in the Task Name column, with the assistance of the ePO SA, identify the weekly on demand client scan task. In the same row as the on demand client scan task, ensure that the Product Name column contains VirusScan Enterprise 8.7.0 and in the Status column, ensure that the status is Enabled. Select Edit from the Actions column. In the Description tab, ensure that for “Type:” “On Demand Scan (VirusScan Enterprise 8.7.0)” is selected. Select the Configuration tab. Under the Scan Locations tab, Scan options area, select “Scan boot sectors”. Select Save.

Group ID (Vulid): V-6602

Group Title: DTAM048-McAfee VirusScan scan all files parameter

Rule ID: SV-21357r1_rule

Severity: CAT II

Rule Version (STIG-ID): DTAM048

Rule Title: The McAfee VirusScan scan all files parameter is not configured as required.

Vulnerability Discussion: This parameter ensures all files are scanned.

Responsibility: System Administrator

Check Content:

From the ePO server console, select Systems tab, select the asset to be checked, select Client Tasks tab. From the list of available tasks in the Task Name column, with the assistance of the ePO SA, identify the weekly on demand client scan task. A daily or weekly on demand client scan may also be identified by reviewing the Product Name, Status, and Schedule of each Task Name in the Client Tasks window. In the same row as the on demand client scan task under review, ensure that the Product Name column contains VirusScan Enterprise 8.7.0 and in the Status column, ensure that the status is Enabled. Select Edit from the Actions column. In the Description tab ensure that for “Type:” “On Demand Scan (VirusScan Enterprise 8.7.0)” is selected. Select the Configuration tab. Under the Scan Items tab, File types to scan: area, ensure that “All files” is selected.

Criteria: If “All files” is selected, this is not a finding.

On the client machine, use the Windows Explorer to navigate to the following folder:

%SystemDrive%\Document and Settings\All Users\Application Data\McAfee\Common Framework\Task\.

Multiple .ini files will be stored in this folder one for each task defined on the ePO server for this client. The name for each task is identified in the first section of the file under the [Task] section on the TaskName= “” line.

Additionally, a TaskType= line in the [General] section of the file is provided to describe the type of scan. In this case, TaskType=VSC700_Scan_Task is expected. Information for this check is determined by examining the

contents of this file.

Criteria: If [What] bScanAllFiles=1, this is not a finding.

Fix Text: From the ePO server console, select Systems tab, select the asset to be checked, select Client Tasks tab. From the list of available tasks in the Task Name column, with the assistance of the ePO SA, identify the weekly on demand client scan task. In the same row as the on demand client scan task, ensure that the Product Name column contains VirusScan Enterprise 8.7.0 and in the Status column, ensure that the status is Enabled. Select Edit from the Actions column. In the Description tab, ensure that for “Type:” “On Demand Scan (VirusScan Enterprise 8.7.0)” is selected. Select the Configuration tab. Under the Scan Items tab, File types to scan: area, select “All files”. Select Save.

Group ID (Vulid): V-6604

Group Title: DTAM050-McAfee VirusScan exclusions parameter

Rule ID: SV-21358r1_rule

Severity: CAT II

Rule Version (STIG-ID): DTAM050

Rule Title: The McAfee VirusScan exclusions parameter is not configured as required.

Vulnerability Discussion: This parameter ensures that there are no exclusions from the virus scanning.

Responsibility: System Administrator

Check Content:

From the ePO server console, select Systems tab, select the asset to be checked, select Client Tasks tab. From the list of available tasks in the Task Name column, with the assistance of the ePO SA, identify the weekly on demand client scan task. A daily or weekly on demand client scan may also be identified by reviewing the Product Name, Status, and Schedule of each Task Name in the Client Tasks window. In the same row as the on demand client scan task under review, ensure that the Product Name column contains VirusScan Enterprise 8.7.0 and in the Status column, ensure that the status is Enabled. Select Edit from the Actions column. In the Description tab, ensure that for “Type:” “On Demand Scan (VirusScan Enterprise 8.7.0)” is selected. Select the Configuration tab. Under the Exclusions tab, “What not to scan:” area, ensure that no items are listed in this area.

Criteria: If no items are listed in the “What not to scan:” area, this is not a finding.

On the client machine, use the Windows Explorer to navigate to the following folder:

%SystemDrive%\Document and Settings\All Users\Application Data\McAfee\Common Framework\Task\.

Multiple .ini files will be stored in this folder one for each task defined on the ePO server for this client. The name for each task is identified in the first section of the file under the [Task] section on the TaskName= “” line.

Additionally, a TaskType= line in the [General] section of the file is provided to describe the type of scan. In this case, TaskType=VSC700_Scan_Task is expected. Information for this check is determined by examining the contents of this file.

Criteria: If [Exclusions] dwExclusionCount=0, this is not a finding.

Fix Text: From the ePO server console, select Systems tab, select the asset to be checked, select Client Tasks tab. From the list of available tasks in the Task Name column, with the assistance of the ePO SA, identify the weekly on demand client scan task. In the same row as the on demand client scan task, ensure that the Product Name column contains VirusScan Enterprise 8.7.0 and in the Status column, ensure that the status is Enabled. Select Edit from the Actions column. In the Description tab, ensure that for “Type:” “On Demand Scan (VirusScan Enterprise 8.7.0)” is selected. Select the Configuration tab. Under the Exclusions tab, “What not to scan:” area, no items should be entered into this area. Select Save.

Group ID (Vulid): V-6611

Group Title: DTAM052-McAfee VirusScan scan archives parameter

Rule ID: SV-21359r1_rule

Severity: CAT II

Rule Version (STIG-ID): DTAM052

Rule Title: The McAfee VirusScan scan archives parameter is not configured as required.

Vulnerability Discussion: This parameter ensures that archive files are checked for viruses.

Responsibility: System Administrator

Check Content:

From the ePO server console, select Systems tab, select the asset to be checked, select Client Tasks tab. From the list of available tasks in the Task Name column, with the assistance of the ePO SA, identify the weekly on demand client scan task. A daily or weekly on demand client scan may also be identified by reviewing the Product Name, Status, and Schedule of each Task Name in the Client Tasks window. In the same row as the on demand client scan task under review, ensure that the Product Name column contains VirusScan Enterprise 8.7.0 and in the Status column, ensure that the status is Enabled. Select Edit from the Actions column. In the Description tab, ensure that for “Type:” “On Demand Scan (VirusScan Enterprise 8.7.0)” is selected. Select the Configuration tab. Under the Scan Items tab, Options: area, ensure that “Scan inside archives (e.g. .ZIP)” is selected.

Criteria: If “Scan inside archives (e.g. .ZIP)” is selected, this is not a finding.

On the client machine, use the Windows Explorer to navigate to the following folder:

%SystemDrive%\Document and Settings\All Users\Application Data\McAfee\Common Framework\Task\.

Multiple .ini files will be stored in this folder one for each task defined on the ePO server for this client. The name for each task is identified in the first section of the file under the [Task] section on the TaskName= “” line.

Additionally, a TaskType= line in the [General] section of the file is provided to describe the type of scan. In this case, TaskType=VSC700_Scan_Task is expected. Information for this check is determined by examining the contents of this file.

Criteria: If [What] ScanArchives=1, this is not a finding.

Fix Text: From the ePO server console, select Systems tab, select the asset to be checked, select Client Tasks tab. From the list of available tasks in the Task Name column, with the assistance of the ePO SA, identify the weekly on demand client scan task. In the same row as the on demand client scan task, ensure that the Product Name column contains VirusScan Enterprise 8.7.0 and in the Status column, ensure that the status is Enabled. Select Edit from the Actions column. In the Description tab, ensure that for “Type:” “On Demand Scan (VirusScan Enterprise 8.7.0)” is selected. Select the Configuration tab. Under the Scan Items tab, Options: area, select “Scan inside archives (e.g. .ZIP)”. Select Save.

Group ID (Vulid): V-6612

Group Title: DTAM053-McAfee VirusScan decode MIME encoded

Rule ID: SV-21360r1_rule

Severity: CAT II

Rule Version (STIG-ID): DTAM053

Rule Title: The McAfee VirusScan decode MIME encoded files parameter is not configured as required.

Vulnerability Discussion: This file ensures that MIME encoded files are scanned for viruses.

Responsibility: System Administrator

Check Content:

From the ePO server console, select Systems tab, select the asset to be checked, select Client Tasks tab. From the list of available tasks in the Task Name column, with the assistance of the ePO SA, identify the weekly on demand client scan task. A daily or weekly on demand client scan may also be identified by reviewing the Product Name, Status, and Schedule of each Task Name in the Client Tasks window. In the same row as the On Demand Client Scan task under review ensure that the Product Name column contains VirusScan Enterprise 8.7.0 and in the Status column, ensure that the status is Enabled. Select Edit from the Actions column. In the Description tab, ensure that for “Type:” “On Demand Scan (VirusScan Enterprise 8.7.0)” is selected. Select the Configuration tab. Under the Scan Items tab, Options: area, ensure that “Decode MIME encoded files” is selected.

Criteria: If “Decode MIME encoded files” is selected, this is not a finding.

On the client machine, use the Windows Explorer to navigate to the following folder:

%SystemDrive%\Document and Settings\All Users\Application Data\McAfee\Common Framework\Task\.

Multiple .ini files will be stored in this folder one for each task defined on the ePO server for this client. The name for each task is identified in the first section of the file under the [Task] section on the TaskName= “” line.

Additionally, a TaskType= line in the [General] section of the file is provided to describe the type of scan. In this case, TaskType=VSC700_Scan_Task is expected. Information for this check is determined by examining the contents of this file.

Criteria: If [What] ScanMIME=1, this is not a finding.

Fix Text: From the ePO server console, select Systems tab, select the asset to be checked, select Client Tasks tab. From the list of available tasks in the Task Name column, with the assistance of the ePO SA, identify the weekly on demand client scan task. In the same row as the On Demand Client Scan task ensure that the Product Name column contains VirusScan Enterprise 8.7.0 and in the Status column, ensure that the status is Enabled. Select Edit from the Actions column. In the Description tab, ensure that for “Type:” “On Demand Scan (VirusScan Enterprise 8.7.0)” is selected. Select the Configuration tab. Under the Scan Items tab, Options: area, select “ScanMime”. Select Save.

Group ID (Vulid): [V-6614](#)

Group Title: DTAM054-McAfee VirusScan find unknown programs

Rule ID: SV-21361r1_rule

Severity: CAT II

Rule Version (STIG-ID): DTAM054

Rule Title: The McAfee VirusScan find unknown programs parameter is not configured as required.

Vulnerability Discussion: This parameter will ensure the virus scanner checks for unknown program viruses.

Responsibility: System Administrator

Check Content:

From the ePO server console, select Systems tab, select the asset to be checked, select Client Tasks tab. From the list of available tasks in the Task Name column, with the assistance of the ePO SA, identify the weekly on demand client scan task. A daily or weekly on demand client scan may also be identified by reviewing the Product Name, Status, and Schedule of each Task Name in the Client Tasks window. In the same row as the on demand client scan task under review, ensure that the Product Name column contains VirusScan Enterprise 8.7.0 and in the Status column, ensure that the status is Enabled. Select Edit from the Actions column. In the Description tab, ensure that for “Type:” “On Demand Scan (VirusScan Enterprise 8.7.0)” is selected. Select the Configuration tab. Under the Scan Items tab, Heuristics: area, ensure that “Find unknown program threats” is selected.

Criteria: If “Find unknown program threats” is selected, this is not a finding.

On the client machine, use the Windows Explorer to navigate to the following folder:

%SystemDrive%\Document and Settings\All Users\Application Data\McAfee\Common Framework\Task\.

Multiple .ini files will be stored in this folder one for each task defined on the ePO server for this client. The name for each task is identified in the first section of the file under the [Task] section on the TaskName= "" line. Additionally, a TaskType= line in the [General] section of the file is provided to describe the type of scan. In this case, TaskType=VSC700_Scan_Task is expected. Information for this check is determined by examining the contents of this file.

Criteria: If [Advanced] dwProgramHeuristicsLevel=1, this is not a finding.

Fix Text: From the ePO server console, select Systems tab, select the asset to be checked, select Client Tasks tab. From the list of available tasks in the Task Name column, with the assistance of the ePO SA, identify the weekly on demand client scan task. In the same row as the on demand client scan task ensure that the Product Name column contains VirusScan Enterprise 8.7.0 and in the Status column, ensure that the status is Enabled. Select Edit from the Actions column. In the Description tab, ensure that for "Type:" "On Demand Scan (VirusScan Enterprise 8.7.0)" is selected. Select the Configuration tab. Under the Scan Items tab, Options: area, select "Find unknown program threats". Select Save.

Group ID (Vulid): V-6615

Group Title: DTAM055-McAfee VirusScan find unknown macro virus

Rule ID: SV-21362r1_rule

Severity: CAT II

Rule Version (STIG-ID): DTAM055

Rule Title: The McAfee VirusScan find unknown macro viruses parameter is not configured as required.

Vulnerability Discussion: This parameter controls checking for unknown macro viruses.

Responsibility: System Administrator

Check Content:

From the ePO server console, select Systems tab, select the asset to be checked, select Client Tasks tab. From the list of available tasks in the Task Name column, with the assistance of the ePO SA, identify the weekly on demand client scan task. A daily or weekly on demand client scan may also be identified by reviewing the Product Name, Status, and Schedule of each Task Name in the Client Tasks window. In the same row as the on demand client scan task under review, ensure that the Product Name column contains VirusScan Enterprise 8.7.0 and in the Status column, ensure that the status is Enabled. Select Edit from the Actions column. In the Description tab, ensure that for "Type:" "On Demand Scan (VirusScan Enterprise 8.7.0)" is selected. Select the Configuration tab. Under the Scan Items tab, Heuristics: area, ensure that "Find unknown macro threats" is selected.

Criteria: If "Find unknown macro threats" is selected, this is not a finding.

On the client machine, use the Windows Explorer to navigate to the following folder:

%SystemDrive%\Document and Settings\All Users\Application Data\McAfee\Common Framework\Task\.

Multiple .ini files will be stored in this folder one for each task defined on the ePO server for this client. The name for each task is identified in the first section of the file under the [Task] section on the TaskName= "" line. Additionally, a TaskType= line in the [General] section of the file is provided to describe the type of scan. In this case, TaskType=VSC700_Scan_Task is expected. Information for this check is determined by examining the contents of this file.

Criteria: If [Advanced] dwMacroHeuristicsLevel=1, this is not a finding.

Fix Text: From the ePO server console, select Systems tab, select the asset to be checked, select Client Tasks tab. From the list of available tasks in the Task Name column, with the assistance of the ePO SA, identify the weekly on demand client scan task. In the same row as the on demand client scan task, ensure that the Product Name column

contains VirusScan Enterprise 8.7.0 and in the Status column, ensure that the status is Enabled. Select Edit from the Actions column. In the Description tab, ensure that for “Type:” “On Demand Scan (VirusScan Enterprise 8.7.0)” is selected. Select the Configuration tab. Under the Scan Items tab, Options: area, select “Find unknown macro threats”. Select Save.

Group ID (Vulid): V-6616

Group Title: DTAM056-McAfee VirusScan action for Virus

Rule ID: SV-21363r1_rule

Severity: CAT II

Rule Version (STIG-ID): DTAM056

Rule Title: The McAfee VirusScan action for Virus parameter is not configured as required.

Vulnerability Discussion: This parameter controls the action when a virus is found.

Responsibility: System Administrator

Check Content:

From the ePO server console, select Systems tab, select the asset to be checked, select Client Tasks tab. From the list of available tasks in the Task Name column, with the assistance of the ePO SA, identify the weekly on demand client scan task. A daily or weekly on demand client scan may also be identified by reviewing the Product Name, Status, and Schedule of each Task Name in the Client Tasks window. In the same row as the on demand client scan task under review, ensure that the Product Name column contains VirusScan Enterprise 8.7.0, in the Status column, ensure that the status is Enabled. Select Edit from the Actions column. In the Description tab, ensure that for “Type:” “On Demand Scan (VirusScan Enterprise 8.7.0)” is selected. Select the Configuration tab. Under the Actions tab, When a threat is found: area, ensure that for the “Perform this action first:” pull down menu, “Clean files” is selected.

Criteria: If “Clean files” is selected, this is not a finding.

On the client machine, use the Windows Explorer to navigate to the following folder:

%SystemDrive%\Document and Settings\All Users\Application Data\McAfee\Common Framework\Task\.

Multiple .ini files will be stored in this folder one for each task defined on the ePO server for this client. The name for each task is identified in the first section of the file under the [Task] section on the TaskName= “” line.

Additionally, a TaskType= line in the [General] section of the file is provided to describe the type of scan. In this case, TaskType=VSC700_Scan_Task is expected. Information for this check is determined by examining the contents of this file.

Criteria: If [Actions] uAction=5, this is not a finding.

Fix Text: From the ePO server console, select Systems tab, select the asset to be checked, select Client Tasks tab. From the list of available tasks in the Task Name column, with the assistance of the ePO SA, identify the weekly on demand client scan task. In the same row as the on demand client scan task, ensure that the Product Name column contains VirusScan Enterprise 8.7.0 and in the Status column, ensure that the status is Enabled. Select Edit from the Actions column. In the Description tab, ensure that for “Type:” “On Demand Scan (VirusScan Enterprise 8.7.0)” is selected. Select the Configuration tab. Under the Actions tab, When a threat is found: area, Perform this action first:, select “Clean files”. Select Save.

Group ID (Vulid): V-6617

Group Title: DTAM057-McAfee VirusScan secondary action

Rule ID: SV-21364r1_rule

Severity: CAT II

Rule Version (STIG-ID): DTAM057

Rule Title: The McAfee VirusScan secondary action for virus parameter is not configured as required.

Vulnerability Discussion: This parameter controls the secondary action that is performed when a virus is found.

Responsibility: System Administrator

Check Content:

From the ePO server console, select Systems tab, select the asset to be checked, select Client Tasks tab. From the list of available tasks in the Task Name column, with the assistance of the ePO SA, identify the weekly on demand client scan task. A daily or weekly on demand client scan may also be identified by reviewing the Product Name, Status, and Schedule of each Task Name in the Client Tasks window. In the same row as the on demand client scan task under review, ensure that the Product Name column contains VirusScan Enterprise 8.7.0 and in the Status column, ensure that the status is Enabled. Select Edit from the Actions column. In the Description tab, ensure that for "Type:" "On Demand Scan (VirusScan Enterprise 8.7.0)" is selected. Select the Configuration tab. Under the Actions tab, When a threat is found: area, ensure that for the "If the first action fails, then perform this action:" pull down menu, "Delete files" is selected.

Criteria: If "Delete files" is selected, this is not a finding.

On the client machine, use the Windows Explorer to navigate to the following folder:

%SystemDrive%\Document and Settings\All Users\Application Data\McAfee\Common Framework\Task\.

Multiple .ini files will be stored in this folder one for each task defined on the ePO server for this client. The name for each task is identified in the first section of the file under the [Task] section on the TaskName= "" line.

Additionally, a TaskType= line in the [General] section of the file is provided to describe the type of scan. In this case, TaskType=VSC700_Scan_Task is expected. Information for this check is determined by examining the contents of this file.

Criteria: If [Actions] uSecAction=4, this is not a finding.

Fix Text: From the ePO server console, select Systems tab, select the asset to be checked, select Client Tasks tab. From the list of available tasks in the Task Name column, with the assistance of the ePO SA, identify the weekly on demand client scan task. In the same row as the on demand client scan task, ensure that the Product Name column contains VirusScan Enterprise 8.7.0 and in the Status column, ensure that the status is Enabled. Select Edit from the Actions column. In the Description tab, ensure that for "Type:" "On Demand Scan (VirusScan Enterprise 8.7.0)" is selected. Select the Configuration tab. Under the Actions tab, When a threat is found: area, If the first action fails, then perform this action:, select "Delete files". Select Save.

Group ID (Vulid): V-6618

Group Title: DTAM059-McAfee VirusScan log to file parameter

Rule ID: SV-21365r1_rule

Severity: CAT II

Rule Version (STIG-ID): DTAM059

Rule Title: The McAfee VirusScan log to file parameter is not configured as required.

Vulnerability Discussion: This parameter ensures that virus scan activities are written to a log file.

Responsibility: System Administrator

Check Content:

From the ePO server console, select Systems tab, select the asset to be checked, select Client Tasks tab. From the list of available tasks in the Task Name column, with the assistance of the ePO SA, identify the weekly on demand client scan task. A daily or weekly on demand client scan may also be identified by reviewing the Product Name, Status, and Schedule of each Task Name in the Client Tasks window. In the same row as the on demand client scan task under review, ensure that the Product Name column, contains VirusScan Enterprise 8.7.0 and in the Status

column, ensure that the status is Enabled. Select Edit from the Actions column. In the Description tab, ensure that for “Type:” “On Demand Scan (VirusScan Enterprise 8.7.0)” is selected. Select the Configuration tab. Under the Reports tab, ensure that for the Log to file: selection “Enable activity logging and accept the default location for the log file or specify a new location” is selected.

Criteria: If “Enable activity logging and accept the default location for the log file or specify a new location” is selected, this is not a finding.

On the client machine, use the Windows Explorer to navigate to the following folder:
 %SystemDrive%\Document and Settings\All Users\Application Data\McAfee\Common Framework\Task\
 Multiple .ini files will be stored in this folder one for each task defined on the ePO server for this client. The name for each task is identified in the first section of the file under the [Task] section on the TaskName= “” line. Additionally, a TaskType= line in the [General] section of the file is provided to describe the type of scan. In this case, TaskType=VSC700_Scan_Task is expected. Information for this check is determined by examining the contents of this file.

Criteria: If [Reports] bLogToFile=1, this is not a finding.

Fix Text: From the ePO server console, select Systems tab, select the asset to be checked, select Client Tasks tab. From the list of available tasks in the Task Name column, with the assistance of the ePO SA, identify the weekly on demand client scan task. In the same row as the on demand client scan task, ensure that the Product Name column contains VirusScan Enterprise 8.7.0 and in the Status column, ensure that the status is Enabled. Select Edit from the Actions column. In the Description tab, ensure that for “Type:” “On Demand Scan (VirusScan Enterprise 8.7.0)” is selected. Select the Configuration tab. Under the Reports tab, for the Log to file: selection, select “Enable activity logging and accept the default location for the log file or specify a new location”. Select Save.

Group ID (Vulid): V-6620

Group Title: DTAM060-McAfee VirusScan log file limit parameter

Rule ID: SV-21366r1_rule

Severity: CAT II

Rule Version (STIG-ID): DTAM060

Rule Title: The McAfee VirusScan log file limit parameter is not configured as required.

Vulnerability Discussion: This parameter determines the minimum size for the log to ensure enough data is available for review.

Responsibility: System Administrator

Check Content:

From the ePO server console, select Systems tab, select the asset to be checked, select Client Tasks tab. From the list of available tasks in the Task Name column, with the assistance of the ePO SA, identify the weekly on demand client scan task. A daily or weekly on demand client scan may also be identified by reviewing the Product Name, Status, and Schedule of each Task Name in the Client Tasks window. In the same row as the on demand client scan task under review, ensure that the Product Name column contains VirusScan Enterprise 8.7.0 and in the Status column, ensure that the status is Enabled. Select Edit from the Actions column. In the Description tab, ensure that for “Type:” “On Demand Scan (VirusScan Enterprise 8.7.0)” is selected. Select the Configuration tab. Under the Reports tab, locate the "Log file size" label.

Criteria: If the "Limit the size of the file" option is not selected, this is not a finding.

Criteria: If the "Limit the size of the file" option is selected, and the “Maximum log file size:” is at least 100MB this is not a finding.

On the client machine, use the Windows Explorer to navigate to the following folder:

%SystemDrive%\Document and Settings\All Users\Application Data\McAfee\Common Framework\Task\.

Multiple .ini files will be stored in this folder one for each task defined on the ePO server for this client. The name for each task is identified in the first section of the file under the [Task] section on the TaskName= "" line.

Additionally, a TaskType= line in the [General] section of the file is provided to describe the type of scan. In this case, TaskType=VSC700_Scan_Task is expected. Information for this check is determined by examining the contents of this file.

Criteria: If [Reports] bLogToFile=1 and [Reports] bLimitSize =>100, this is not a finding.

Fix Text: From the ePO server console, select Systems tab, select the asset to be checked, select Client Tasks tab. From the list of available tasks in the Task Name column, with the assistance of the ePO SA, identify the weekly on demand client scan task. In the same row as the on demand client scan task, ensure that the Product Name column contains VirusScan Enterprise 8.7.0 and in the Status column, ensure that the status is Enabled. Select Edit from the Actions column. In the Description tab, ensure that for "Type:" "On Demand Scan (VirusScan Enterprise 8.7.0)" is selected. Select the Configuration tab. Under the Reports tab, locate the "Log file size:" label. If the "Limit the size of the file" option is not to be used, ensure "Limit the size of the file" is not selected. If the "Limit the size of the file" option is selected, ensure the "Maximum log file size:" is at least 100MB. Select Save.

Group ID (Vulid): V-6621

Group Title: DTAM061-McAfee VirusScan log session settings

Rule ID: SV-21368r1_rule

Severity: CAT II

Rule Version (STIG-ID): DTAM061

Rule Title: The McAfee VirusScan log session settings parameter is not configured as required.

Vulnerability Discussion: This parameter ensures that session settings are logged.

Responsibility: System Administrator

Check Content:

From the ePO server console, select Systems tab, select the asset to be checked, select Client Tasks tab. From the list of available tasks in the Task Name column, with the assistance of the ePO SA, identify the weekly on demand client scan task. A daily or weekly on demand client scan may also be identified by reviewing the Product Name, Status, and Schedule of each Task Name in the Client Tasks window. In the same row as the on demand client scan task under review, ensure that the Product Name column contains VirusScan Enterprise 8.7.0 and in the Status column, ensure that the status is Enabled. Select Edit from the Actions column. In the Description tab, ensure that for "Type:" "On Demand Scan (VirusScan Enterprise 8.7.0)" is selected. Select the Configuration tab. Under the Reports tab, locate the "What to log in addition to scanning activity" label.

Criteria: If the "Session settings" option is selected, this is not a finding.

On the client machine, use the Windows Explorer to navigate to the following folder:

%SystemDrive%\Document and Settings\All Users\Application Data\McAfee\Common Framework\Task\.

Multiple .ini files will be stored in this folder one for each task defined on the ePO server for this client. The name for each task is identified in the first section of the file under the [Task] section on the TaskName= "" line.

Additionally, a TaskType= line in the [General] section of the file is provided to describe the type of scan. In this case, TaskType=VSC700_Scan_Task is expected. Information for this check is determined by examining the contents of this file.

Criteria: If [Reports] bLogSettings=1, this is not a finding.

Fix Text: From the ePO server console, select Systems tab, select the asset to be checked, select Client Tasks tab. From the list of available tasks in the Task Name column, with the assistance of the ePO SA, identify the weekly on demand client scan task. In the same row as the on demand client scan task, ensure that the Product Name column contains VirusScan Enterprise 8.7.0 and in the Status column, ensure that the status is Enabled. Select Edit from the Actions column. In the Description tab, ensure that for "Type:" "On Demand Scan (VirusScan Enterprise 8.7.0)" is selected. Select the Configuration tab. Under the Reports tab, locate the "What to log in addition to scanning activity:" label. Select Session settings. Select Save.

Group ID (Vulid): V-6624

Group Title: DTAM062-McAfee VirusScan log session summary

Rule ID: SV-21369r1_rule

Severity: CAT II

Rule Version (STIG-ID): DTAM062

Rule Title: The McAfee VirusScan log session summary parameter is not configured as required.

Vulnerability Discussion: This parameter ensures that session summary information is logged for future review if needed.

Responsibility: System Administrator

Check Content:

From the ePO server console, select Systems tab, select the asset to be checked, select Client Tasks tab. From the list of available tasks in the Task Name column, with the assistance of the ePO SA, identify the weekly on demand client scan task. A daily or weekly on demand client scan may also be identified by reviewing the Product Name, Status, and Schedule of each Task Name in the Client Tasks window. In the same row as the on demand client scan task under review, ensure that the Product Name column contains VirusScan Enterprise 8.7.0 and in the Status column, ensure that the status is Enabled. Select Edit from the Actions column. In the Description tab, ensure that for "Type:" "On Demand Scan (VirusScan Enterprise 8.7.0)" is selected. Select the Configuration tab. Under the Reports tab, locate the "What to log in addition to scanning activity" label.

Criteria: If the "Session summary" option is selected, this is not a finding.

On the client machine, use the Windows Explorer to navigate to the following folder:

%SystemDrive%\Document and Settings\All Users\Application Data\McAfee\Common Framework\Task\.

Multiple .ini files will be stored in this folder one for each task defined on the ePO server for this client. The name for each task is identified in the first section of the file under the [Task] section on the TaskName= "" line.

Additionally, a TaskType= line in the [General] section of the file is provided to describe the type of scan. In this case, TaskType=VSC700_Scan_Task is expected. Information for this check is determined by examining the contents of this file.

Criteria: If [Reports] bLogSummary=1, this is not a finding.

Fix Text: From the ePO server console, select Systems tab, select the asset to be checked, select Client Tasks tab. From the list of available tasks in the Task Name column, with the assistance of the ePO SA, identify the weekly on demand client scan task. In the same row as the on demand client scan task, ensure that the Product Name column contains VirusScan Enterprise 8.7.0 and in the Status column, ensure that the status is Enabled. Select Edit from the Actions column. In the Description tab, ensure that for "Type:" "On Demand Scan (VirusScan Enterprise 8.7.0)" is selected. Select the Configuration tab. Under the Reports tab, locate the "What to log in addition to scanning activity:" label. Select Session summary. Select Save.

Group ID (Vulid): V-6625

Group Title: DTAM063-McAfee VirusScan failure on encrypted file

Rule ID: SV-21370r1_rule

Severity: CAT II

Rule Version (STIG-ID): DTAM063

Rule Title: The McAfee VirusScan failure on encrypted files parameter is not configured as required.

Vulnerability Discussion: This parameter ensures that failures on encrypted files are logged.

Responsibility: System Administrator

Check Content:

From the ePO server console, select Systems tab, select the asset to be checked, select Client Tasks tab. From the list of available tasks in the Task Name column, with the assistance of the ePO SA, identify the weekly on demand client scan task. A daily or weekly on demand client scan may also be identified by reviewing the Product Name, Status, and Schedule of each Task Name in the Client Tasks window. In the same row as the on demand client scan task under review, ensure that the Product Name column contains VirusScan Enterprise 8.7.0 and in the Status column, ensure that the status is Enabled. Select Edit from the Actions column. In the Description tab, ensure that for "Type:" "On Demand Scan (VirusScan Enterprise 8.7.0)" is selected. Select the Configuration tab. Under the Reports tab, locate the "What to log in addition to scanning activity" label.

Criteria: If the "Failure to scan encrypted files" option is selected, this is not a finding.

On the client machine, use the Windows Explorer to navigate to the following folder:

%SystemDrive%\Document and Settings\All Users\Application Data\McAfee\Common Framework\Task\.

Multiple .ini files will be stored in this folder one for each task defined on the ePO server for this client. The name for each task is identified in the first section of the file under the [Task] section on the TaskName= "" line.

Additionally, a TaskType= line in the [General] section of the file is provided to describe the type of scan. In this case, TaskType=VSC700_Scan_Task is expected. Information for this check is determined by examining the contents of this file.

Criteria: If [Reports] bLogScanFailure=1, this is not a finding.

Fix Text: From the ePO server console, select Systems tab, select the asset to be checked, select Client Tasks tab. From the list of available tasks in the Task Name column, with the assistance of the ePO SA, identify the weekly on demand client scan task. In the same row as the on demand client scan task, ensure that the Product Name column contains VirusScan Enterprise 8.7.0 and in the Status column, ensure that the status is Enabled. Select Edit from the Actions column. In the Description tab, ensure that for "Type:" "On Demand Scan (VirusScan Enterprise 8.7.0)" is selected. Select the Configuration tab. Under the Reports tab, locate the "What to log in addition to scanning activity:" label. Select Failure to scan encrypted files. Select Save.

Group ID (Vulid): V-6627

Group Title: DTAM070-McAfee VirusScan schedule

Rule ID: SV-21379r1_rule

Severity: CAT II

Rule Version (STIG-ID): DTAM070

Rule Title: The McAfee VirusScan schedule is not configured as required.

Vulnerability Discussion: This parameter ensures that a comprehensive On-Demand system virus scan is scheduled to be executed on at least a weekly basis.

Responsibility: System Administrator

Check Content:

From the ePO server console, select Systems tab, select the asset to be checked, select Client Tasks tab. From the list of available tasks in the Task Name column, with the assistance of the ePO SA, identify the weekly on demand client scan task. A daily or weekly on demand client scan may also be identified by reviewing the Product Name, Status, and Schedule of each Task Name in the Client Tasks window. In the same row as the on demand client scan task under review, ensure that the Product Name column contains VirusScan Enterprise 8.7.0 and in the Status column, ensure that the status is Enabled. Select Edit from the Actions column. In the Description tab, ensure that for "Type:" "On Demand Scan (VirusScan Enterprise 8.7.0)" is selected. Select the Schedule tab. In the "Schedule Status:" area, ensure Enabled is selected. Also, in the Schedule type: area (using the pull down menu), ensure that the scan is scheduled for at least a weekly scan.

Criteria: If the Scheduled status: is Enabled and the Schedule type: is at least weekly, this is not a finding.

On the client machine, use the Windows Explorer to navigate to the following folder:

%SystemDrive%\Document and Settings\All Users\Application Data\McAfee\Common Framework\Task\.

Multiple .ini files will be stored in this folder one for each task defined on the ePO server for this client. The name for each task is identified in the first section of the file under the [Task] section on the TaskName= "" line.

Additionally, a TaskType= line in the [General] section of the file is provided to describe the type of scan. In this case, TaskType=VSC700_Scan_Task is expected. Information for this check is determined by examining the contents of this file.

Criteria:

If [Settings] Enabled=1 and [Schedule] Type=0 the schedule is daily, this is not a finding.

If [Settings] Enabled=1 and [Schedule] Type=1 the schedule is weekly, this is not a finding.

Fix Text: From the ePO server console, select Systems tab, select the asset to be checked, select Client Tasks tab. From the list of available tasks in the Task Name column, with the assistance of the ePO SA, identify the weekly on demand client scan task. In the same row as the on demand client scan task, ensure that the Product Name column contains VirusScan Enterprise 8.7.0 and in the Status column, ensure that the status is Enabled. Select Edit from the Actions column. In the Description tab, ensure that for "Type:" "On Demand Scan (VirusScan Enterprise 8.7.0)" is selected. Select the Schedule tab. In the "Schedule Status:" area select Enabled, in the Schedule type: area (using the pull down menu), ensure that the scan is scheduled on at least a weekly basis.

Group ID (Vulid): V-14618

Group Title: DTAM090-McAfee VirusScan onaccess scan scripts

Rule ID: SV-21382r1_rule

Severity: CAT II

Rule Version (STIG-ID): DTAM090

Rule Title: The McAfee VirusScan on access scan parameter for script scan is incorrect.

Vulnerability Discussion: ScriptScan analyzes each webpage opened on your computer via Outlook or a web browser for JavaScript and VBScript. If an unwanted script is found it is not allowed to execute.

Responsibility: System Administrator

Check Content:

From the ePO server console, select Systems tab, select the asset to be checked, select the Policies tab, select from the product pull down list VirusScan Enterprise 8.7.0. Locate in the Category column the On-Access General Policies. Select from the Policy column the policy associated with the On-Access General Policies. Under the ScriptScan tab, locate the "ScriptScan:" label. Ensure the "Enable scanning of scripts" option is selected.

Criteria: If the "Enable scanning of scripts" option is selected, this is not a finding.

Check Content:

Procedure: Use the Windows Registry Editor to navigate to the following key:

HKLM\Software\McAfee\VSCore\Script Scanner

Criteria: If the value of ScriptScanEnabled is 1, this is not a finding.

Fix Text: From the ePO server console, select Systems tab, select the asset to be checked, select the Policies tab, select from the product pull down list VirusScan Enterprise 8.7.0. Locate in the Category column the On-Access General Policies. Select from the Policy column the policy associated with the On-Access General Policies. Under the ScriptScan tab, locate the "ScriptScan:" label. Select the "Enable scanning of scripts" option. Select Save.

Group ID (Vulid): [V-14619](#)

Group Title: DTAM091-McAfee VirusScan onaccess scan blocking

Rule ID: SV-21386r1_rule

Severity: CAT II

Rule Version (STIG-ID): DTAM091

Rule Title: The McAfee VirusScan on access scan parameter for connection blocking is incorrect.

Vulnerability Discussion: This setting is required to block connections from remote computers when a threat or unwanted program is detected in a shared folder.

Responsibility: System Administrator

Check Content:

From the ePO server console, select Systems tab, select the asset to be checked, select the Policies tab, select from the product pull down list VirusScan Enterprise 8.7.0. Locate in the Category column the On-Access General Policies. Select from the Policy column the policy associated with the On-Access General Policies. Under the Blocking tab, locate the "Block the connection:" label. Ensure the "Block the connection when a threatened file is detected in a shared folder" option is selected.

Criteria: If the "Block the connection when a threatened file is detected in a shared folder" option is selected, this is not a finding.

Check Content:

Procedure: Use the Windows Registry Editor to navigate to the following key:

HKLM\Software\McAfee\VSCore\On Access Scanner\BehaviourBlocking

Criteria: If the value of VSIDBlock is 1, this is not a finding.

Fix Text: From the ePO server console, select Systems tab, select the asset to be checked, select the Policies tab, select from the product pull down list VirusScan Enterprise 8.7.0. Locate in the Category column the On-Access General Policies. Select from the Policy column the policy associated with the On-Access General Policies. Under the Blocking tab, locate the "Block the connection:" label. Select the "Block the connection when a threatened file is detected in a shared folder" option.

Group ID (Vulid): [V-14620](#)

Group Title: DTAM092-McAfee VirusScan onaccess scan blocking

Rule ID: SV-21400r1_rule

Severity: CAT II

Rule Version (STIG-ID): DTAM092

Rule Title: The McAfee VirusScan on access scan parameter for connection blocking time is incorrect.

Vulnerability Discussion: This parameter unblocks suspected threats in a remote computer shared connection. If a threat is detected blocking blocks the connection. This parameter unblocks the connection after at minimum of 30 minutes.

Responsibility: System Administrator

Check Content:

From the ePO server console, select Systems tab, select the asset to be checked, select the Policies tab, select from the product pull down list VirusScan Enterprise 8.7.0. Locate in the Category column the On-Access General Policies. Select from the Policy column the policy associated with the On-Access General Policies. Under the Blocking tab, locate the "Block the connection:" label. Ensure the "Unblock connections after x minutes" where x is set to no less than 30 minutes.

Criteria: If the "Unblock connections after 30 minutes" option is selected, this is not a finding.

Check Content:

Procedure: Use the Windows Registry Editor to navigate to the following key:

HKLM\Software\McAfee\VSCore\On Access Scanner\BehaviourBlocking

Criteria: If the value of VSIDBlockTimeout >= to HEX 1E, this is not a finding.

Fix Text: From the ePO server console, select Systems tab, select the asset to be checked, select the Policies tab, select from the product pull down list VirusScan Enterprise 8.7.0. Locate in the Category column the On-Access General Policies. Select from the Policy column the policy associated with the On-Access General Policies. Under the Blocking tab, locate the "Block the connection:" label. Set the "Unblock connections after x minutes", where x is set to no less than 30 minutes.

Group ID (Vulid): [V-14621](#)

Group Title: DTAM093-McAfee VirusScan onaccess scan blocking

Rule ID: SV-21404r1_rule

Severity: CAT II

Rule Version (STIG-ID): DTAM093

Rule Title: The McAfee VirusScan on access scan parameter for blocking unwanted programs is incorrect.

Vulnerability Discussion: This setting blocks the connection to a remote computer share where an unwanted program is found in the remote share folder.

Responsibility: System Administrator

Check Content:

From the ePO server console, select Systems tab, select the asset to be checked, select the Policies tab, select from the product pull down list VirusScan Enterprise 8.7.0. Locate in the Category column the On-Access General Policies. Select from the Policy column the policy associated with the On-Access General Policies. Under the Blocking tab, locate the "Block the connection:" label. Ensure the "Unblock connections after x minutes", where x is set to no less than 30 minutes.

Criteria: If the "Unblock connections after =>30 minutes" option is selected, this is not a finding.

Check Content:

Procedure: Use the Windows Registry Editor to navigate to the following key:

HKLM\Software\McAfee\VSCore\On Access Scanner\BehaviourBlocking

Criteria: If the value of VSIDBlockOnNonVirus is 1, this is not a finding.

Fix Text: From the ePO server console, select Systems tab, select the asset to be checked, select the Policies tab, select from the product pull down list VirusScan Enterprise 8.7.0. Locate in the Category column the On-Access General Policies. Select from the Policy column the policy associated with the On-Access General Policies. Under

the Blocking tab, locate the "Block the connection:" label. Set the "Unblock connections after x minutes", where x is set to no less than 30 minutes.

Group ID (Vulid): [V-14622](#)

Group Title: DTAM100-McAfee VirusScan scan default values

Rule ID: SV-21405r1_rule

Severity: CAT II

Rule Version (STIG-ID): DTAM100

Rule Title: The McAfee VirusScan scan default values for processes are not configured as required.

Vulnerability Discussion: With this setting set to "Configure one scanning policy for all processes" one policy baseline for all on-access scanning is set using one set of policy options.

Responsibility: System Administrator

Check Content:

From the ePO server console, select Systems tab, select the asset to be checked, select the Policies tab, select from the product pull down list VirusScan Enterprise 8.7.0. Locate in the Category column the On-Access Default Policies. Select from the Policy column the policy associated with the On-Access Default Policies. Under the Processes tab, locate the "Process Settings:" label. Ensure the "Configure one scanning policy for all processes" is selected.

Criteria: If the "Configure one scanning policy for all processes" option is selected, this is not a finding.

Check Content:

Procedure: Use the Windows Registry Editor to navigate to the following key:

HKLM\software\McAfee\VSCore\On Access Scanner\McShield\Configuration

Criteria: If the value OnlyUseDefaultConfig is 1, this is not a finding.

Fix Text: From the ePO server console, select Systems tab, select the asset to be checked, select the Policies tab, select from the product pull down list VirusScan Enterprise 8.7.0. Locate in the Category column the On-Access Default Policies. Select from the Policy column the policy associated with the On-Access Default Policies. Under the Processes tab, locate the "Process Settings:" label. Select the "Configure one scanning policy for all processes" option. Select Save.

Group ID (Vulid): [V-14623](#)

Group Title: DTAM101-McAfee VirusScan scan when writing disk

Rule ID: SV-21406r1_rule

Severity: CAT II

Rule Version (STIG-ID): DTAM101

Rule Title: The McAfee VirusScan scan when writing to disk is not configured as required.

Vulnerability Discussion: This setting requires on-access scanning to be performed whenever a files is written to a non-networked disk drive.

Responsibility: System Administrator

Check Content:

Procedure: Use the Windows Registry Editor to navigate to the following key:

HKLM\software\McAfee\VSCore\On Access Scanner\McShield\Configuration\default

Criteria: If the value bScanIncoming is 1, this is not a finding.

Check Content:

From the ePO server console, select Systems tab, select the asset to be checked, select the Policies tab, select from the product pull down list VirusScan Enterprise 8.7.0. Locate in the Category column the On-Access Default Policies. Select from the Policy column the policy associated with the On-Access Default Policies. Under the Scan Items tab, locate the "Scan files label. Ensure the "When writing to disk" is selected.

Criteria: If the "When writing to disk" option is selected, this is not a finding.

Fix Text: From the ePO server console, select Systems tab, select the asset to be checked, select the Policies tab, select from the product pull down list VirusScan Enterprise 8.7.0. Locate in the Category column the On-Access Default Policies. Select from the Policy column the policy associated with the On-Access Default Policies. Under the Scan Items tab, locate the "Scan files:" label. Select the "When writing to disk" option. Select Save.

Group ID (Vulid): V-14624

Group Title: DTAM102-McAfee VirusScan scan when reading

Rule ID: SV-21407r1_rule

Severity: CAT II

Rule Version (STIG-ID): DTAM102

Rule Title: The McAfee VirusScan scan when reading parameter is not configured as required.

Vulnerability Discussion: This setting requires on-access scanning to be performed whenever a files are read from a non-networked disk drive.

Responsibility: System Administrator

Check Content:

Procedure: Use the Windows Registry Editor to navigate to the following key:

HKLM\software\McAfee\VSCore\On Access Scanner\McShield\Configuration\default

Criteria: If the value bScanOutgoing is 1, this is not a finding.

Check Content:

From the ePO server console, select Systems tab, select the asset to be checked, select the Policies tab, select from the product pull down list VirusScan Enterprise 8.7.0. Locate in the Category column the On-Access Default Policies. Select from the Policy column the policy associated with the On-Access Default Policies. Under the Scan Items tab, locate the "Scan files label. Ensure the "When reading from disk" is selected.

Criteria: If the "When reading from disk" option is selected, this is not a finding.

Fix Text: From the ePO server console, select Systems tab, select the asset to be checked, select the Policies tab, select from the product pull down list VirusScan Enterprise 8.7.0. Locate in the Category column the On-Access Default Policies. Select from the Policy column the policy associated with the On-Access Default Policies. Under the Scan Items tab, locate the "Scan files:" label. Select the "When reading from disk" option. Select Save.

Group ID (Vulid): V-14625

Group Title: DTAM103-McAfee VirusScan scan all files parameter

Rule ID: SV-21409r1_rule

Severity: CAT II

Rule Version (STIG-ID): DTAM103

Rule Title: The McAfee VirusScan scan all files parameter is not configured as required.

Vulnerability Discussion: This setting requires on-access scanning to be performed whenever a file is read from or written to network drives.

Responsibility: System Administrator

Check Content:

From the ePO server console, select Systems tab, select the asset to be checked, select the Policies tab, select from the product pull down list VirusScan Enterprise 8.7.0. Locate in the Category column the On-Access Default Policies. Select from the Policy column the policy associated with the On-Access Default Policies. Under the Scan Items tab, locate the "Scan files label. Ensure the "On network drives" is selected.

Criteria: If the "On network drives" option is selected, this is not a finding.

Check Content:

Procedure: Use the Windows Registry Editor to navigate to the following key:

HKLM\software\McAfee\VSCore\On Access Scanner\McShield\Configuration\default

Criteria: If the value LocalExtensionMode is 1 and the value of NetworkExtensionMode is 1 this is not a finding. If either of these is not 1, this is a finding.

Fix Text: From the ePO server console, select Systems tab, select the asset to be checked, select the Policies tab, select from the product pull down list VirusScan Enterprise 8.7.0. Locate in the Category column the On-Access Default Policies. Select from the Policy column the policy associated with the On-Access Default Policies. Under the Scan Items tab, locate the "Scan files:" label. Select the "On network drives" option. Select Save.

Group ID (Vulid): [V-14626](#)

Group Title: DTAM104-McAfee VirusScan heuristics program

Rule ID: SV-21410r1_rule

Severity: CAT II

Rule Version (STIG-ID): DTAM104

Rule Title: The McAfee VirusScan heuristics program viruses parameter is not configured as required.

Vulnerability Discussion: This setting requires on-access scanning to "Find unknown program threats and trojans" based on heuristic problem solving techniques.

Responsibility: System Administrator

Check Content:

From the ePO server console, select Systems tab, select the asset to be checked, select the Policies tab, select from the product pull down list VirusScan Enterprise 8.7.0. Locate in the Category column the On-Access Default Policies. Select from the Policy column the policy associated with the On-Access Default Policies. Under the Scan Items tab, locate the "Heuristics:" label. Ensure the "Find unknown program threats and trojans" option is selected.

Criteria: If the "Find unknown program threats and trojans" option is selected, this is not a finding.

Check Content:

Procedure: Use the Windows Registry Editor to navigate to the following key:

HKLM\software\McAfee\VSCore\On Access Scanner\McShield\Configuration\default

Criteria: If the value dwProgramHeuristicsLevel is 1, this is not a finding.

Fix Text: From the ePO server console, select Systems tab, select the asset to be checked, select the Policies tab, select from the product pull down list VirusScan Enterprise 8.7.0. Locate in the Category column the On-Access Default Policies. Select from the Policy column the policy associated with the On-Access Default Policies. Under the Scan Items tab, locate the "Heuristics:" label. Select the "Find unknown program threats and trojans" option. Select save.

Group ID (Vulid): V-14627

Group Title: DTAM105-McAfee VirusScan heuristics macro level

Rule ID: SV-21411r1_rule

Severity: CAT II

Rule Version (STIG-ID): DTAM105

Rule Title: The McAfee VirusScan heuristics macro viruses parameter is not configured as required.

Vulnerability Discussion: This setting requires on-access scanning to "Find unknown macro threats" based on heuristic problem solving techniques.

Responsibility: System Administrator

Check Content:

From the ePO server console, select Systems tab, select the asset to be checked, select the Policies tab, select from the product pull down list VirusScan Enterprise 8.7.0. Locate in the Category column the On-Access Default Policies. Select from the Policy column the policy associated with the On-Access Default Policies. Under the Scan Items tab, locate the "Heuristics:" label. Ensure the "Find unknown macro threats" option is selected.

Criteria: If the "Find unknown macro threats" option is selected, this is not a finding.

Check Content:

Procedure: Use the Windows Registry Editor to navigate to the following key:

HKLM\software\McAfee\VSCore\On Access Scanner\McShield\Configuration\default

Criteria: If the value dwMacroHeuristicsLevel is 1, this is not a finding.

Fix Text: From the ePO server console, select Systems tab, select the asset to be checked, select the Policies tab, select from the product pull down list VirusScan Enterprise 8.7.0. Locate in the Category column the On-Access Default Policies. Select from the Policy column the policy associated with the On-Access Default Policies. Under the Scan Items tab, locate the "Heuristics:" label. Select the "Find unknown macro threats" option. Select save.

Group ID (Vulid): V-14628

Group Title: DTAM106-McAfee VirusScan scan inside archive

Rule ID: SV-21412r1_rule

Severity: CAT II

Rule Version (STIG-ID): DTAM106

Rule Title: The McAfee VirusScan scan inside archives parameter is not configured as required.

Vulnerability Discussion: This setting requires on-access scanning to scan inside archive files such as .ZIP files. This also enables on-access scanning to be performed on other compressed file types as well.

Responsibility: System Administrator

Check Content:

From the ePO server console, select Systems tab, select the asset to be checked, select the Policies tab, select from the product pull down list VirusScan Enterprise 8.7.0. Locate in the Category column the On-Access Default Policies. Select from the Policy column the policy associated with the On-Access Default Policies. Under the Scan Items tab, locate the "Compressed files:" label. Ensure the "Scan inside archives (e.g. .ZIP)" option is selected.

Criteria: If the "Scan inside archives (e.g. .ZIP)" option is selected, this is not a finding.

Check Content:

Procedure: Use the Windows Registry Editor to navigate to the following key:

HKLM\software\McAfee\VSCore\On Access Scanner\McShield\Configuration\default

Criteria: If the value ScanArchives is 1, this is not a finding.

Fix Text: From the ePO server console, select Systems tab, select the asset to be checked, select the Policies tab, select from the product pull down list VirusScan Enterprise 8.7.0. Locate in the Category column the On-Access Default Policies. Select from the Policy column the policy associated with the On-Access Default Policies. Under the Scan Items tab, locate the "Compressed files:" label. Select the "Scan inside archives (e.g. .ZIP)" option. Select Save.

Group ID (Vulid): V-14629

Group Title: DTAM107-McAfee VirusScan scan MIME files parameter

Rule ID: SV-21413r1_rule

Severity: CAT II

Rule Version (STIG-ID): DTAM107

Rule Title: The McAfee VirusScan scan MIME files parameter is not configured as required.

Vulnerability Discussion: This setting requires on-access scanning to decode and scan Multipart Internet Mail Extension (MIME) encoded files.

Responsibility: System Administrator

Check Content:

From the ePO server console, select Systems tab, select the asset to be checked, select the Policies tab, select from the product pull down list VirusScan Enterprise 8.7.0. Locate in the Category column the On-Access Default Policies. Select from the Policy column the policy associated with the On-Access Default Policies. Under the Scan Items tab, locate the "Compressed files:" label. Ensure the "Decode MIME encoded files" option is selected.

Criteria: If the "Decode MIME encoded files" option is selected, this is not a finding.

Check Content:

Procedure: Use the Windows Registry Editor to navigate to the following key:

HKLM\software\McAfee\VSCore\On Access Scanner\McShield\Configuration\default

Criteria: If the value ScanMime is 1, this is not a finding.

Fix Text: From the ePO server console, select Systems tab, select the asset to be checked, select the Policies tab, select from the product pull down list VirusScan Enterprise 8.7.0. Locate in the Category column the On-Access Default Policies. Select from the Policy column the policy associated with the On-Access Default Policies. Under the Scan Items tab, locate the "Compressed files:" label. Select the "Decode MIME encoded files" option. Select Save.

Group ID (Vulid): V-14630

Group Title: DTAM110-McAfee VirusScan process primary action

Rule ID: SV-21414r1_rule

Severity: CAT II

Rule Version (STIG-ID): DTAM110

Rule Title: The McAfee VirusScan process primary action parameter is not configured as required.

Vulnerability Discussion: This setting requires that for On-Access scanning the first response to a threat that is detected is to "Clean files automatically".

Responsibility: System Administrator

Check Content:

From the ePO server console, select Systems tab, select the asset to be checked, select the Policies tab, select from

the product pull down list VirusScan Enterprise 8.7.0. Locate in the Category column the On-Access Default Policies. Select from the Policy column the policy associated with the On-Access Default Policies. Under the Actions tab, When a threat is found: area, ensure that for the “Perform this action first:” pull down menu, “Clean files” is selected.

Criteria: If “Clean files” is selected, this is not a finding.

Check Content:

Procedure: Use the Windows Registry Editor to navigate to the following key:

HKLM\software\McAfee\VSCore\On Access Scanner\McShield\Configuration\default

Criteria: If the value UAction_Program is 4 this is not a finding.

Fix Text: From the ePO server console, select Systems tab, select the asset to be checked, select the Policies tab, select from the product pull down list VirusScan Enterprise 8.7.0. Locate in the Category column the On-Access Default Policies. Select from the Policy column the policy associated with the On-Access Default Policies. Under the Actions tab, in When a threat is found: area, Perform this action first:, select “Clean files”. Select Save.

Group ID (Vulid): V-14631

Group Title: DTAM111-McAfee VirusScan process secondary action

Rule ID: SV-21415r1_rule

Severity: CAT II

Rule Version (STIG-ID): DTAM111

Rule Title: The McAfee VirusScan process secondary action parameter is not configured as required.

Vulnerability Discussion: This setting is required in response to a threat that could not be cleaned by the On-Access "Clean Files Automatically" setting. In this event the On_access setting for "If the first action fails, then perform this action:" is "Delete Files Automatically". If the file cannot be repaired it should be deleted.

Responsibility: System Administrator

Check Content:

From the ePO server console, select Systems tab, select the asset to be checked, select the Policies tab, select from the product pull down list VirusScan Enterprise 8.7.0. Locate in the Category column the On-Access Default Policies. Select from the Policy column the policy associated with the On-Access Default Policies. Under the Actions tab, When a threat is found: area, ensure that for the “If the first action fails, then perform this action:” pull down menu, “Delete files” is selected.

Criteria: If “Delete files” is selected, this is not a finding.

Check Content:

Procedure: Use the Windows Registry Editor to navigate to the following key:

HKLM\software\McAfee\VSCore\On Access Scanner\McShield\Configuration\default

Criteria: If the value USecAction_Program is 5 this is not a finding. If the value is 0, this is a finding.

Fix Text: From the ePO server console, select Systems tab, select the asset to be checked, select the Policies tab, select from the product pull down list VirusScan Enterprise 8.7.0. Locate in the Category column the On-Access Default Policies. Select from the Policy column the policy associated with the On-Access Default Policies. Under the Actions tab, When a threat is found: area, If the first action fails, then perform this action:, select “Delete files”. Select Save.

Group ID (Vulid): V-14651

Group Title: DTAM038-McAfee VirusScan detect unwanted program

Rule ID: SV-21416r1_rule

Severity: CAT II

Rule Version (STIG-ID): DTAM038

Rule Title: The McAfee VirusScan detects unwanted programs email parameter is not configured as required.

Vulnerability Discussion: This setting is required for the On-Delivery Email scan. This settings enables the detection of unwanted programs to include Malware and Spyware.

Responsibility: System Administrator

Check Content:

From the ePO server console, select Systems tab, select the asset to be checked, select the Policies tab, select from the product pull down list VirusScan Enterprise 8.7.0. Locate in the Category column the On Delivery Email Scan Policies. Select from the Policy column the policy associated with the On Delivery Email Scan Policies. Under the Scan Items tab, locate the "Unwanted programs detection:" label. Ensure the "Detect unwanted programs" option is selected.

Criteria: If the option "Detect unwanted programs" is selected, this is not a finding.

Check Content:

Procedure: Use the Windows Registry Editor to navigate to the following key:

HKLM\software\McAfee\VSCore\Email Scanner\Outlook\OnDelivery\DetectionOptions

Criteria: If the value ApplyNVP is 1, this is not a finding.

Fix Text: From the ePO server console, select Systems tab, select the asset to be checked, select the Policies tab, select from the product pull down list VirusScan Enterprise 8.7.0. Locate in the Category column the On Delivery Email Scan Policies. Select from the Policy column the policy associated with the On Delivery Email Scan Policies. Under the Scan Items tab, locate the "Unwanted programs detection:" label. Select the "Detect unwanted programs" option.

Group ID (Vulid): V-14652

Group Title: DTAM039-McAfee VirusScan unwanted programs action

Rule ID: SV-21417r1_rule

Severity: CAT II

Rule Version (STIG-ID): DTAM039

Rule Title: The McAfee VirusScan unwanted programs action email parameter is not configured as required.

Vulnerability Discussion: This setting is required for the On Delivery Email Scan Policies. When an unwanted program is found the first action to be performed is the "Prompt for action" option. At that time the option to delete, clean, or archive the program is presented to the user.

Responsibility: System Administrator

Check Content:

From the ePO server console, select Systems tab, select the asset to be checked, select the Policies tab, select from the product pull down list VirusScan Enterprise 8.7.0. Locate in the Category column the On Delivery Email Scan Policies. Select from the Policy column the policy associated with the On Delivery Email Scan Policies. Under the Actions tab, locate the "When an unwanted program is found:" section. In the "Perform this action first:" pull down menu, select the "Prompt for action" option. Select save.

Criteria: If the option "Prompt for action" is selected, this is not a finding.

Check Content:

Procedure: Use the Windows Registry Editor to navigate to the following key:

HKLM\software\McAfee\VSCore\Email Scanner\Outlook\OnDelivery\ActionOptions

Criteria: If the value uAction_Program is 2, this is not a finding.

Fix Text: From the ePO server console, select Systems tab, select the asset to be checked, select the Policies tab, select from the product pull down list VirusScan Enterprise 8.7.0. Locate in the Category column the On Delivery Email Scan Policies. Select from the Policy column the policy associated with the On Delivery Email Scan Policies. Under the Actions tab, locate the "When an unwanted program is found:" section. In the "Perform this action first:" pull down menu, select the "Prompt for action" option. Select save.

Group ID (Vulid): [V-14654](#)

Group Title: DTAM058-McAfee VirusScan check unwanted programs

Rule ID: SV-21418r1_rule

Severity: CAT II

Rule Version (STIG-ID): DTAM058

Rule Title: The McAfee VirusScan check for unwanted programs parameter is not configured as required.

Vulnerability Discussion: This setting enables the detection of unwanted programs during a scheduled, On-Demand Scan, scan. The "Detect unwanted programs" option is required to be selected in the configuration for the daily or weekly On Demand Scan.

Responsibility: System Administrator

Check Content:

From the ePO server console, select Systems tab, select the asset to be checked, select Client Tasks tab. From the list of available tasks in the Task Name column, with the assistance of the ePO SA, identify the weekly on demand client scan task. A daily or weekly on demand client scan may also be identified by reviewing the Product Name, Status, and Schedule of each Task Name in the Client Tasks window. In the same row as the on demand client scan task under review, ensure that the Product Name column contains VirusScan Enterprise 8.7.0 and in the Status column, ensure that the status is Enabled. Select Edit from the Actions column. In the Description tab, ensure that for "Type:" "On Demand Scan (VirusScan Enterprise 8.7.0)" is selected. Select the Configuration tab. Under the Scan Items tab, Options: area, ensure that "Detect unwanted programs" is selected.

Criteria: If "Detect unwanted programs" is selected in the configuration for the daily or weekly On Demand Scan, this is not a finding.

On the client machine, use the Windows Explorer to navigate to the following folder:

%SystemDrive%\Document and Settings\All Users\Application Data\McAfee\Common Framework\Task\.

Multiple .ini files will be stored in this folder one for each task defined on the ePO server for this client. The name for each task is identified in the first section of the file under the [Task] section on the TaskName= "" line.

Additionally, a TaskType= line in the [General] section of the file is provided to describe the type of scan. In this case, TaskType=VSC700_Scan_Task is expected. Information for this check is determined by examining the contents of this file.

Criteria: If [Spyware] ApplyNVP=1 is present, this is not a finding.

Fix Text: From the ePO server console, select Systems tab, select the asset to be checked, select Client Tasks tab. From the list of available tasks in the Task Name column, with the assistance of the ePO SA, identify the weekly on demand client scan task. In the same row as the on demand client scan task, ensure that the Product Name column contains VirusScan Enterprise 8.7.0 and in the Status column, ensure that the status is Enabled. Select Edit from the

Actions column. In the Description tab, ensure that for "Type:" "On Demand Scan (VirusScan Enterprise 8.7.0)" is selected. Select the Configuration tab. Under the Scan Items tab, Options: area, select "Detect unwanted programs". Select Save.

Group ID (Vulid): [V-14657](#)

Group Title: DTAM130-McAfee VirusScan buffer overflow protectio

Rule ID: SV-21419r1_rule

Severity: CAT II

Rule Version (STIG-ID): DTAM130

Rule Title: The McAfee VirusScan buffer overflow protection is not configured as required.

Vulnerability Discussion: This setting is required to ensure that buffer overflow protection is enabled. Buffer overflow protection prevents tampered with application code from being executed on the computer.

Responsibility: System Administrator

Check Content:

From the ePO server console, select Systems tab, select the asset to be checked, select the Policies tab, select from the product pull down list VirusScan Enterprise 8.7.0. Locate in the Category column the Buffer Overflow Protection Policies. Select from the Policy column the policy associated with the Buffer Overflow Protection Policies. Under the Buffer Overflow Protection tab, locate the "Buffer Overflow settings:" label. Ensure the "Enable buffer overflow protection" option is selected.

Criteria: If the "Enable buffer overflow protection" option is selected, this is not a finding.

Check Content:

Procedure: Use the Windows Registry Editor to navigate to the following key:
HKLM\Software\McAfee\VSCore\On Access Scanner\BehaviourBlocking

Criteria: If the value BOPEnabled is 1, this is not a finding.

Fix Text: From the ePO server console, select Systems tab, select the asset to be checked, select the Policies tab, select from the product pull down list VirusScan Enterprise 8.7.0. Locate in the Category column the Buffer Overflow Protection Policies. Select from the Policy column the policy associated with, in the same row as, the Buffer Overflow Protection Policies. Under the Buffer Overflow Protection tab, locate the "Buffer Overflow settings:" label. Select the "Enable buffer overflow protection" option. Select Save.

Group ID (Vulid): [V-14658](#)

Group Title: DTAM131-McAfee VirusScan buffer overflow protectio

Rule ID: SV-21420r1_rule

Severity: CAT II

Rule Version (STIG-ID): DTAM131

Rule Title: The McAfee VirusScan buffer overflow protection mode is not configured as required.

Vulnerability Discussion: This setting is required to ensure that buffer overflow protection is enabled and that "Protection mode" is enabled. Buffer overflow protection prevents tampered with application code from being executed on the computer. The "Protection mode" option is selected to ensure that the application is prevented from executing.

Responsibility: System Administrator

Check Content:

From the ePO server console, select Systems tab, select the asset to be checked, select the Policies tab, select from the product pull down list VirusScan Enterprise 8.7.0. Locate in the Category column the Buffer Overflow Protection Policies. Select from the Policy column the policy associated with the Buffer Overflow Protection Policies. Under the Buffer Overflow Protection tab, locate the "Buffer Overflow settings:" label. Ensure the "Protection mode" option is selected.

Criteria: If the "Protection mode" option is selected, this is not a finding.

Check Content:

Procedure: Use the Windows Registry Editor to navigate to the following key:
HKLM\Software\McAfee\VSCore\On Access Scanner\BehaviourBlocking

Criteria: Set the value BOPMode to 1.

Fix Text: From the ePO server console, select Systems tab, select the asset to be checked, select the Policies tab, select from the product pull down list VirusScan Enterprise 8.7.0. Locate in the Category column the Buffer Overflow Protection Policies. Select from the Policy column the policy associated with the Buffer Overflow Protection Policies. Under the Buffer Overflow Protection tab, locate the "Buffer Overflow settings:" label. Select the "Protection mode" option. Select Save.

Group ID (Vulid): [V-14659](#)

Group Title: DTAM132-McAfee VirusScan buffer overflow message

Rule ID: SV-21421r1_rule

Severity: CAT II

Rule Version (STIG-ID): DTAM132

Rule Title: The McAfee VirusScan buffer overflow message parameter is not configured as required.

Vulnerability Discussion: This setting is required to ensure when buffer overflow protection is enabled that the "Show the messages dialog box when a buffer overflow is detected" is selected. Buffer overflow protection prevents tampered with application code from being executed on the computer. The "Show the messages dialog box when a buffer overflow is detected" option is selected to ensure that the user is notified .

Responsibility: System Administrator

Check Content:

From the ePO server console, select Systems tab, select the asset to be checked, select the Policies tab, select from the product pull down list VirusScan Enterprise 8.7.0. Locate in the Category column the Buffer Overflow Protection Policies. Select from the Policy column the policy associated with the Buffer Overflow Protection Policies. Under the Buffer Overflow Protection tab, locate the "Client system warning:" label. Ensure the "Show the messages dialog box when a buffer overflow is detected" option is selected.

Criteria: If the "Show the messages dialog box when a buffer overflow is detected" option is selected, this is not a finding.

Check Content:

Procedure: Use the Windows Registry Editor to navigate to the following key:
HKLM\Software\McAfee\VSCore\On Access Scanner\BehaviourBlocking

Criteria: If the value BOPShowMessages is 1, this is not a finding.

Fix Text: From the ePO server console, select Systems tab, select the asset to be checked, select the Policies tab, select from the product pull down list VirusScan Enterprise 8.7.0. Locate in the Category column the Buffer Overflow Protection Policies. Select from the Policy column the policy associated with the Buffer Overflow

Protection Policies. Under the Buffer Overflow Protection tab, locate the "Client system warning:" label. Select the "Show the messages dialog box when a buffer overflow is detected" option. Select Save.

Group ID (Vulid): [V-14660](#)

Group Title: DTAM133-McAfee VirusScan buffer overflow log

Rule ID: SV-21422r1_rule

Severity: CAT II

Rule Version (STIG-ID): DTAM133

Rule Title: The McAfee VirusScan buffer overflow log parameter is not configured as required.

Vulnerability Discussion: This setting is required to ensure when buffer overflow protection is enabled that the "Enable activity logging and accept the default location for the log file or specify a new location" is selected. Buffer overflow protection prevents tampered with application code from being executed on the computer. The "Enable activity logging and accept the default location for the log file or specify a new location" option is selected to ensure that buffer overflow logging is being performed .

Responsibility: System Administrator

Check Content:

From the ePO server console, select Systems tab, select the asset to be checked, select the Policies tab, select from the product pull down list VirusScan Enterprise 8.7.0. Locate in the Category column the Buffer Overflow Protection Policies. Select from the Policy column the policy associated with the Buffer Overflow Protection Policies. Under the Reports tab, locate the "Log to file:" label.

Criteria: If the "Enable activity logging and accept the default location for the log file or specify a new location" option is selected, this is not a finding.

Check Content:

Procedure: Use the Windows Registry Editor to navigate to the following key:

HKLM\software\McAfee\VSCore\On Access Scanner\BehaviourBlocking

Criteria: If the value bLogToFile_Ent is 1, this is not a finding.

Fix Text: From the ePO server console, select Systems tab, select the asset to be checked, select the Policies tab, select from the product pull down list VirusScan Enterprise 8.7.0. Locate in the Category column the Buffer Overflow Protection Policies. Select from the Policy column the policy associated with the Buffer Overflow Protection Policies. Under the Reports tab, locate the "Log to file:" label. Select the "Enable activity logging and accept the default location for the log file or specify a new location" option. Select Save.

Group ID (Vulid): [V-14661](#)

Group Title: DTAM134-McAfee VirusScan log size limitation

Rule ID: SV-21423r1_rule

Severity: CAT II

Rule Version (STIG-ID): DTAM134

Rule Title: The McAfee VirusScan log size limitation parameters are not configured as required.

Vulnerability Discussion: This setting is required to ensure when buffer overflow protection is enabled that the "Log file size" is selected. Buffer overflow protection prevents tampered with application code from being executed on the computer. The "Log file size" option is selected to ensure that buffer overflow log file size does not exceed 100mb.

Responsibility: System Administrator

Check Content:

From the ePO server console, select Systems tab, select the asset to be checked, select the Policies tab, select from the product pull down list VirusScan Enterprise 8.7.0. Locate in the Category column the Buffer Overflow Protection Policies. Select from the Policy column the policy associated with the Buffer Overflow Protection Policies. Under the Reports tab, locate the "Log file size" label.

Criteria: If the "Limit the size of the file" option is not selected, this is not a finding.

Criteria: If the "Limit the size of the file" option is selected, ensure the "Maximum log file size:" is at least 100MB.

Check Content:

Procedure: Use the Windows Registry Editor to navigate to the following key:

HKLM\software\McAfee\VSCore\On Access Scanner\BehaviourBlocking

Criteria: If the value bLimitSize_Ent is 1 and the value of dwMaxLogSizeMB_Ent is at least x40 (64), this is not a finding.

Fix Text: From the ePO server console, select Systems tab, select the asset to be checked, select the Policies tab, select from the product pull down list VirusScan Enterprise 8.7.0. Locate in the Category column the Buffer Overflow Protection Policies. Select from the Policy column the policy associated with the Buffer Overflow Protection Policies. Under the Reports tab, locate the "Log file size:" label. If the "Limit the size of the file" option is not to be used ensure "Limit the size of the file" is not selected. If the "Limit the size of the file" option is selected, ensure the "Maximum log file size:" is at least 100MB.

Group ID (Vulid): [V-14662](#)

Group Title: DTAM135-McAfee VirusScan detection of Spyware

Rule ID: SV-21424r1_rule

Severity: CAT II

Rule Version (STIG-ID): DTAM135

Rule Title: The McAfee VirusScan detection of Spyware is not configured as required.

Vulnerability Discussion: This setting is required to ensure that under the Unwanted Programs Policies, Spyware is selected. This enables the detection of Spyware on the system.

Responsibility: System Administrator

Check Content:

From the ePO server console, select Systems tab, select the asset to be checked, select the Policies tab, select from the product pull down list VirusScan Enterprise 8.7.0. Locate in the Category column the Unwanted Programs Policies. Select the policy associated with the Unwanted Programs Policies. Under the Scan Items tab, locate the "Select categories of unwanted programs to detect:" label. Ensure the "Spyware" option is selected.

Criteria: If the "Spyware" option is selected, this is not a finding.

Check Content:

Procedure: Use the Windows Registry Editor to navigate to the following key:

HKLM\software\McAfee\VSCore\NVP

Criteria: If the value DetectSpyware is 1, this is not a finding.

Fix Text: From the ePO server console, select Systems tab, select the asset to be checked, select the Policies tab, select from the product pull down list VirusScan Enterprise 8.7.0. Locate in the Category column the On-Access Default Policies. Select from the Policy column the policy associated with the On-Access Default Policies. Under the Scan Items tab, locate the "Select categories of unwanted programs to detect:" label. Select the "Spyware" option. Select Save.

Group ID (Vulid): [V-14663](#)

Group Title: DTAM136-McAfee VirusScan detection of Adware

Rule ID: SV-21426r1_rule

Severity: CAT II

Rule Version (STIG-ID): DTAM136

Rule Title: The McAfee VirusScan detection of Adware is not configured as required.

Vulnerability Discussion: This setting is required to ensure that under the Unwanted Programs Policies, Adware is selected. This enables the detection of Adware on the system.

Responsibility: System Administrator

Check Content:

From the ePO server console, select Systems tab, select the asset to be checked, select the Policies tab, select from the product pull down list VirusScan Enterprise 8.7.0. Locate in the Category column the Unwanted Programs Policies. Select the policy associated with the Unwanted Programs Policies. Under the Scan Items tab, locate the "Select categories of unwanted programs to detect:" label. Ensure the "Adware" option is selected.

Criteria: If the "Adware" option is selected, this is not a finding.

Check Content:

Procedure: Use the Windows Registry Editor to navigate to the following key:

HKLM\software\McAfee\VSCore\NVP

Criteria: If the value DetectAdware is 1, this is not a finding.

Fix Text: From the ePO server console, select Systems tab, select the asset to be checked, select the Policies tab, select from the product pull down list VirusScan Enterprise 8.7.0. Locate in the Category column the On-Access Default Policies. Select from the Policy column the policy associated with the On-Access Default Policies. Under the Scan Items tab, locate the "Select categories of unwanted programs to detect:" label. Select the "Adware" option. Select Save.

Group ID (Vulid): [V-19910](#)

Group Title: Virus Signature Files older than 7 days.

Rule ID: SV-22090r1_rule

Severity: CAT I

Rule Version (STIG-ID): DTAG008

Rule Title: The antivirus signature file age exceeds 7 days.

Vulnerability Discussion: Antivirus signature files are updated almost daily by antivirus software vendors. These files are made available to antivirus clients as they are published. Keeping virus signature files as current as possible is vital to the security of any system.

Note: If the vendor or trusted site's files match the date of the signature files on the machine, this is not a finding.

Responsibility: System Administrator

Check Content:

On client machine locate McAfee icon in system tray. Right click to open and choose VirusScan Console. Select Help then choose About VirusScan Enterprise. Displayed will be a date for "DAT Created On:". Criteria: If the "DAT Created On:" date is older than 7 calendar days from the current date, this is a finding.

Note: If the vendor or trusted site's files are also older than 7 days and match the date of the signature files on the

machine, this is not a finding.

Fix Text: Update client machines via ePo. If this fails to update the client, update antivirus signature file as your local process describes e.g autoupdate or runtime executable.

UNCLASSIFIED